جامعة نايف العربية للعلوم الأمنية

مركز
الدراسات
والبحوث

وعي المواطن العربي تجاه جرائم الاحتيال

«بطاقات الدفع الإلكتروني نموذجاً»

اللواء . نجاح محمد فوزي

الريـــاض
١٤٢٨هـ ـ ٢٠٠٧م

٤٢٦

جامعة نايف العربية للعلوم الأمنية

وعي المواطن العربي تجاه جرائم الاحتيال

«بطاقات الدفع الإلكتروني نموذجاً»

اللواء . نجاح محمد فوزي

الريـــاض
١٤٢٨هـ ـ ٢٠٠٧م

(٢٠٠٧)، جامعة نايف العربية للعلوم الأمنية ـ الرياض ـ
المملكة العربية السعودية. ص. ب ٦٨٣٠ الرياض: ١١٤٥٢
هاتف ٢٤٦٣٤٤٤ (ـ١ـ٩٦٦) فاكس ٢٤٦٤٧١٣ (ـ١ـ٩٦٦)
البريد الإلكتروني: Src@nauss.edu.sa

ISBN 3 - 9 - 9902 - 9960- 978

P.O.Box: 6830 Riyadh 11452 Tel. (966+1) 2463444 KSA
Fax (966 + 1) 2464713 E-mail Src@nauss.edu.sa.

(١٤٢٨هـ)جامعة نايف العربية للعلوم الأمنية
فهرسة مكتبة الملك فهد الوطنية أثناء النشر

فوزي، نجاح محمد
وعي المواطن العربي تجاه جرائم الاحتيال: بطاقات الدفع الإلكتروني نموذجاً، ـ الرياض، ١٤٢٨هـ
٢٠٢ص، ١٧ × ٢٤ سم
ردمك: ٣ ـ ٩ ـ ٩٩٠٢ ـ ٩٩٦٠ ـ ٩٧٨
١ ـ النصب والاحتيال ٢ ـ بطاقات الائتمان أ ـ العنوان
ديوي ٣٦٤,١٦٣ ١٤٢٨/٤٥٣٧

رقم الايداع: ١٤٢٨/٤٥٣٧
ردمك: ٣ ـ ٩ ـ ٩٩٠٢ ـ ٩٩٦٠ ـ ٩٧٨

المحتويـــات

التقديـــم

تعد البطاقات الائتمانية من أهم مظاهر التطور التي حدثت في البيئة الاقتصادية في العصر الحديث الذي اتسم بسرعة التغيرات التي واكبت التقدم التكنولوجي لوسائل الاتصال.

وقد غدت البطاقات الائتمانية تلعب دوراً مهماً وأساسياً في الائتمان والمعاملات التجارية والمصرفية على مستوى الأفراد والمؤسسات الرسمية والخاصة.

وإن المتأمل للكم الهائل من الأشخاص الذين يستخدمون البطاقات الائتمانية بعد أن قدمت البنوك كثيراً من التسهيلات التي تشجع على امتلاكها واستخدامها يدرك مدى سهولة استخدام تلك البطاقات وأهميتها في المعاملات التجارية والمصرفية سواء أكان ذلك من قبل مستخدمها أو المستفيد منها أو التاجر أو البائع القابل للبطاقة، ويدرك أيضاً خطورة التساهل في استخدامها من قبل الآخرين أو تزويرها عند السرقة أو الفقدان.

ومن هنا فقد جاءت أهمية هذه (الدراسة) التي ألقت الضوء على الأخطار التي تواجه مستخدمي البطاقات الائتمانية وأساليب مواجهة تلك الأخطار بعد أن ظهرت أشكال إجرامية متجددة اتخذت من نظم الدفع الإلكتروني وسطاً مناسباً لأساليب التزوير والاحتيال والسرقة تمثلت في استخدام البطاقات المسروقة أو المفقودة، أو استصدار بطاقات صحيحة بمستندات مزورة، أو تزوير إشعارات المبيعات المستخدمة مع نظام الدفع الإلكتروني، أو تواطؤ بعض التجار أو التلاعب في أجهزة البيع الإلكتروني... وغيرها من الأساليب.

وأن جامعة نايف العربية للعلوم الأمنية إذ تنشر هذه (الدراسة) ضمن سلسلة إصداراتها التوعوية لترجو أن تكون إضافة جديدة إلى المكتبة الأمنية العربية وترجو أن يكون فيها ما يؤكد أهمية حرص المواطن العربي على حسن استخدام البطاقات الائتمانية وحسن الاستفادة من إيجابياتها بعيداً عن التلاعب في استخدامها أو الوقوع في براثن جرائم الاحتيال.

والله من وراء القصد، ، ،

رئيس

جامعة نايف العربية للعلوم الأمنية

أ. د. عبد العزيز بن صقر الغامدي

المقدمـــة

منذ العصور القديمة لجأ الإنسان لاستخدام العديد من وسائل التبادل، ففي البداية اتخذ المعادن وسيطاً للمبادلات، ومنها المعادن النفيسة، ثم اهتدي بعد ذلك للمسكوكات، وهى عبارة عن قطع من المعدن النفيس محددة الوزن ومنقوش على وجهها قيمتها والدولة المصدرة لها، وبعد تعرض المسكوكات للغش بالإضافة لعدم ثبات قيمتها لكونها تتأثر دوماً بأسعار الذهب، ظهرت الأوراق النقدية لتلعب دوراً هاماً في الحياة التجارية، وبظهورها بدأ الإنسان يبحث عن وسيلة لتأمينها من الأخطار التي تتعرض لها مثل السرقة والضياع، وأيضا وسيلة لانتقالها من مكان إلى آخر، ومن يد إلى يد، وهنا ظهرت البنوك لتؤدي دورها الذى ظل يتطور حتى يومنا هذا[1].

وفي ظل الطفرات المذهلة التي حققتها ثورة المعلومات والاتصالات تعيش البشرية اليوم ظروفاً اقتصادية واجتماعية جعلت من شعوب العالم كياناً واحداً كادت أن تتلاشى معه حدود الدول.

وفي ظل تلك الثورة أيضا تعاظم دور البنوك والمصارف وباتت تشارك في كافة الأنشطة الاجتماعية والاقتصادية، وكنتيجة لتنوع الخدمات التي تؤديها زاد عملاؤها حتى أصبحت جزءاً هاماً من الكيان الاقتصادي لأي مجتمع، كما أصبحنا نرى مؤسسات مالية تمارس نشاطها عبر قارات الدنيا في ظل طفرة نظم الاتصالات الحديثة، حتى إنه لا توجد مؤسسة مالية اليوم يمكن أن تمارس نشاطها بمعزل عن تلك المنظومة، وأصبحت الثروات تنتقل

---

(١) محمد حافظ الرهوان، النقود والبنوك والأسواق المالية، القاهرة، ٢٠٠٠ م، ص ٥٣.

من دولة لأخرى، ومن عملة لأخرى بنبضات إلكترونية، في ظل ما يسمى بالعمليات المصرفية الإلكترونية.

بدائل النقود وتطور وسائل السداد

وكان من الطبيعى أن يصاحب تطور الأنشطة المصرفية ظهور بدائل للنقود مثل الشيكات بأنواعها «شخصية، مصرفية، سياحية» والتحويلات البنكية Banking Wiretransfer وأوامر الدفع المصرفية وكذا السندات الاذنية، وظهرت بطاقات الدفع لأول مرة عام ١٩٥١ بمعرفة مؤسسة داينرز كلوب Diners Club بالولايات المتحدة الأمريكية وانتشرت خارجها.

وقد اكتسبت بطاقات الدفع الخاصية الاليكترونية في بداية السبعينات من القرن الماضى في ظل التطور الذى لحق بنظم الاتصالات والمعلومات، كما ساعد انتشار شبكة الانترنت الهائل خلال العقدين الماضيين على تطور استخدام تلك البطاقات في الحياة اليومية، فأصبح بإمكان أي مواطن شراء أي شئ من أي مكان في العالم طوال أيام الأسبوع وعلى مدار الأربع والعشرين ساعة ودون الحاجة إلى مبارحة مكانه.

السداد من خلال الهاتف المحمول M-Commerce

وتعنى إمكانية استخدام الأجهزة المحمولة كالمساعد الرقمى الشخصى PDA والتليفون المحمول كوسيلة لتسديد قيمة ما يحصل عليه الفرد من معلومات أو خدمات أو سلع، ومن المتوقع أن تحدث هذه الخدمة ثورة هائلة في نمط الحياة اليومية خلال السنوات القليلة القادمة[١].

---

(١) فى فنلندا «على سبيل المثال» أتاحت هذه الخدمة للسائقين إمكانية دفع قيمة غسيل سياراتهم دون الحاجة إلى الخروج منها، وفى دبى تم تركيب ماكينات خاصة فى كافة أنحاء المدينة خلال مهرجان التسوق عام ٢٠٠٥ لتمكين المتسوقين من شراء =

السداد ببصمة الإصبع Pay By Tuch

أعلنت مؤخراً إحدى المؤسسات المالية بالمملكة المتحدة عن إتاحة خدمة السداد ببصمة الإصبع لدى بعض المتاجر والمطاعم في ثلاث مقاطعات إنجليزية، حيث يقوم المشتري بملامسة إصبعه مع النهاية الطرفية الإلكترونية لدى التاجر ـ POS ـ المتصلة بشبكة المعلومات لدى البنك ليتم خصم قيمة المشتريات من حساب المشتري ودون الحاجة لحمل النقود أو بطاقة الدفع أو حتى أية وسيلة أخرى لإثبات الشخصية[1].

وكما هو الحال دائماً، سيتمثل التحدي الرئيس في كيفية إطلاق قوى التكنولوجيا من أجل خير البشرية، وفي الوقت نفسه لابد من بذل الجهود لمنع إساءة استغلالها.

فقد كان من الطبيعى أن تظهر أشكال إجرامية جديدة اتخذت من تلك النظم المصرفية والمعلوماتية وسطاً هائلاً للنمو والانتشار، فكما رأينا التعليم عن بعد، والتسوق عن بعد والاشتراك في المؤتمرات والندوات عن بعد، إذ بنا نرى أيضا الجرائم التي ترتكب عن بعد.

= المشروبات عن طريق رسائل قصيرة SMS من خلال هواتفهم المحمولة راجع كتيب «مجتمع اللانقود» من إصدارات مكتبة منظمة الفيزا العالمية، بالقاهرة عام ٢٠٠٦ ص ١٥.

وراجع أيضا موقع كل من: منظمة الفيزhttp://www.visa.com. ومنظمةGSM - http://www.gsmworld.com

(١) تطبق هذه الخدمة من خلال ما يعرف بالتكنولوجيا البيومترية Biometric Technology وتعنى التعرف على الأشخاص وتحديد الهوية عن طريق الخصائص الحيوية مثل بصمات الإصبع أو الأذن أو العين أو عظام الوجه، راجع موقع http:/ /www.complicanceandprivacy.com.

فقد أتاح انتشار استخدام وتطور بطاقات الدفع الاليكتروني الفرصة لمحترفي جرائم الاحتيال المعلوماتى لارتكاب جرائهم متخذين وسائل المراوغة والتخفي ما يجعلهم بمنأى عن الملاحقة أو الضبط .

ويرى مسئولو الأخطار بالمؤسسات المالية الدولية المعنية ببطاقات الدفع الإليكترونى مثل فيزا Visa ، ماستر كارد Master Card أن جرائم بطاقات الدفع الإليكترونى تعد من أكثر أنواع جرائم الاحتيال نمواً في العالم وذلك للأسباب التالية :

١ ـ سهولة السفر والتنقل إلى مختلف بلدان العالم وتطور نظم المعلومات والاتصالات .

٢ ـ ضعف التعاون بين أجهزة المكافحة في مختلف الدول من جهة وبين السلطات القضائية في هذه الدول من جهة أخرى .

٣ ـ ارتفاع العائدات المتحصلة من هذه الأنشطة ، في ظل عدم اهتمام نسبة كبيرة من حاملى البطاقات بمراجعة كشوف الحساب الشهرية التي ترد إليهم من بنوكهم .

٤ ـ ضعف التعاون الدولى في مواجهة تلك الأنشطة .

٥ ـ انعدام وجود تشريعات عقابية متخصصة لمحاربة هذا النوع من الجرائم في العديد من الدول .

وتجدر بنا الإشارة إلى أن استجابة المشرعين في مختلف الدول لمواجهة هذا النوع من الجرائم ، وكذا جرائم تكنولوجيا المعلومات ، تختلف باختلاف درجة التقدم العلمى في هذه الدول أو تلك ، ففي الدول المتقدمة تكنولوجياً واجه المشرعون هذه الجرائم المستحدثة بقوانين خاصة تتضمن

عقوبات تتناسب مع درجة خطورتها[1]، بينما خلت التشريعات العقابية لمعظم البلدان العربية من أية نصوص صريحة تجرم الأفعال غير المشروعة المصاحبة لنشاط بطاقات الدفع الإليكترونى « باستثناء كل من قطر وسلطنة عمان » اكتفاء بنصوص المواد العقابية المتعلقة بجرائم السرقة والتزوير والاحتيال و خيانة الأمانة .

هجرة جرائم بطاقات الدفع الإليكترونى

وقد رصد مسئولو الأخطار بالمؤسسات المالية الدولية المعنية ظاهرة هجرة بعض الأنماط الإجرامية لبطاقات الدفع الإليكترونى «خاصة تلك المرتبطة بتكنولوجيا المعلومات » من الدول المتقدمة إلى الدول الأقل تقدماً، في ظل اهتمام السلطات والمؤسسات المالية في تلك الدول بوضع التدابير التشريعية والأمنية والحلول الفنية في مواجهة هذا النوع من الجرائم .

وتشير المعلومات إلى أن بعض مجموعات الجريمة المنظمة كثيراً ما تستغل تلك الثغرات، حيث تلجأ إلى عمليات الاحتيال ببطاقات الدفع لتمويل أنواع أخرى من الجرائم منها الإرهاب وتهريب المخدرات والأفلام الإباحية وتهريب الأشخاص وتجارة الأسلحة[2] .

وإذا كان الهدف من هذه الدراسة هو إلقاء الضوء على هذا النوع من الجرائم ووضع تصور لكيفية مواجهتها، فإنه يجب علينا أن ندق ناقوس الخطر من الآن، فالمواجهة السريعة لهذا النوع من الجرائم يجب أن تكون

---

(١) جميل عبد الباقي الصغير ، الإنترنت والقانون الجنائى ، دار نهضة مصر ، ٢٠٠١م، ص ١٠ .

(٢) وسام عابد ، الاحتيال الإليكترونى فن ومحاربته علم ، ورقة عمل مقدمة لمؤتمر مستقبل الدفع الإليكترونى ، دبى مارس ٢٠٠٦ .

من خلال ثلاثة محاور رئيسية ـ تشريعية وأمنية وفنية ـ ولا يخفى في هذا المقام الدور الذى يجب أن يقوم به رجال إنقاذ القانون سواء من الشرطة أو القضاء، لذا كان الارتقاء بهم والعمل على رفع كفاءتهم وتأهيلهم فنيا وميدانياً أمراً حتمياً.

وتعد هذه الدراسة وصفية تحليلية، انتهجنا فيها بالمنهج الوصفي الذي يسعى إلى وصف وتشخيص موضوع البحث من مختلف جوانبه وأبعاده.

وقد اعتمدنا في جمع مادة هذه الدراسة على العديد من المصادر منها:

١ ـ عدد من الكتب العلمية القانونية المتخصصة.

٢ ـ بعض الدراسات والبحوث السابقة.

٣ ـ أرشيف الإدارة العامة لمباحث الأموال العامة بوزارة الداخلية. جمهورية مصر العربية.

٤ ـ وبرغم أن هناك اتجاهاً داخل الأوساط العلمية بعدم الاستناد إلى مواقع شبكة الإنترنت كمراجع في البحوث المختلفة « لاتصاف أغلب تلك المواقع بعدم الثبات وتعرض المحتوى للتغيير المستمر» إلا أن ارتباط جانب كبير من جرائم بطاقات الدفع الإليكترونى بإستخدامات تلك الشبكة العجيبة، قد فرض علينا الرجوع إلى العديد من المواقع المتخصصة، خاصة مواقع بعض المنظمات الدولية وأجهزة المكافحة لدى بعض الدول الغربية التي سبقتنا في هذا المجال.

٥ ـ وأخيرا الخبرة الميدانية التي اكتسبناها في مكافحة هذا النوع من الجرائم على مدى أكثر من عشرين عاماً، والاحتكاك بالخبرات الأجنبية من خلال المشاركة في فرق العمل والمؤتمرات والندوات المختلفة.

وقد تناولنا هذا الموضوع في خمسة فصول، فتحدثنا في الفصل الأول «الذى صار بمثابة فصل تمهيدي» عن خصائص جرائم الاحتيال وتطورها، ثم تحدثنا عن بطاقات الدفع الإلكتروني من حيث النشأة والتطور وآليات العمل في الفصل الثانى، أما في الفصل الثالث فقد أفردناه لتحديد أخطار هذا النوع من البطاقات وفي الفصل الرابع تناولنا كيفية مواجهته وأخيرا فقد جاء الفصل الخامس ليكون بمثابة الجانب التطبيقى لهذه الدراسة من خلال عرض لنماذج مختلفة من جرائم بطاقات الدفع الإليكترونى والقضايا التي تم ضبطها في هذا المجال.

وقد انتهينا من دراستنا إلى مجموعة من النتائج والتوصيات آملين أن تجد صدى لدى كل من يعّن له الأمر في مواجهة تحديات المستقبل.

والله ولى التوفيق، ،

الباحث

الفصل الأول

خصائص جرائم الاحتيال وتطورها

١ .خصائص جرائم الاحتيال وتطورها

تتميز جرائم الاحتيال بوجود علاقة طردية بين المحتال والضحية ومحورها الوعى والثقافة » فكلما زاد الوعى ومستوى العلم لدى المحتال وانخفض لدى الضحية تمكن الأول من الثانى .

وكثيرا ما يكون للمجني عليه في هذا النوع من الجرائم دور في تهيئة الفرصة الإجرامية للجاني ، وذلك لأسباب كثيرة ، أهمها انخفاض المستوي العلمي والثقافي ، والطمع وحسن النية المفرط ، وعدم توخي الحرص لدى التعامل مع الآخرين . . . الخ .

وقد انتشرت جرائم الاحتيال في المجتمعات العربية وتنوعت أشكالها ، كما تأثرت بالتطور التكنولوجي فظهر الاحتيال العابر للحدود . .

لذا فإننا سنتناول بالدراسة خصائص جرائم الاحتيال وتطورها في أقسام ثلاثة . . ففي القسم الأول نتحدث عن خصائص هذا النوع من الجرائم بينما نتحدث في القسم الثاني عن أهم وأكثر جرائم الاحتيال انتشاراً في المجتمعات العربية أما في الثالث فنتحدث عن (الاحتيالات المالية عبر شبكة الإنترنت) .

١ .١ خصائص الاحتيال

تطورت جرائم الاحتيال في المجتمعات العربية مع تطور العلاقات الاجتماعية وتشابكها خلال العقود الماضية ، فكانت صورة المحتال الراسخة في الأذهان هي لذلك الشخص الذي يقف داخل المحطة النهائية للقطار أو للحافلات داخل مدينة من المدن الكبرى لاصطياد ضحية من بين القرويين

القادمين للمدينة بحثاً عن الرزق، ليستولى على ما بحوزتهم من نقود معدودة.

ومع بداية عصر ثورة المعلومات تغيرت الصورة الذهنية لذلك المحتال، وظهرت أنماط إجرامية جديدة، تنوعت معها جرائم الاحتيال وتنوعت أساليبها، فمنها ما استهدف الأفراد ومنها ما استهدف أموال شركات ومؤسسات كبرى، ومع ظهور شبكة الانترنت وتنامي استخداماتها ظهرت أشكال احتيالية جديدة اتخذت من بيئة هذه الشبكة مناخاً خصباً تنمو فيه، ولم تقتصر جرائم الاحيتال على المستوى المحلى فقط، بل تخطت آثارها حدود الدول دون حائل يمنعها.

ويتميز هذا النوع من الجرائم بطبيعة خاصة، حيث تستهدف الأفعال المادية فيها العبث بخيال الضحية لحمله على تحقيق مآرب المحتال طواعية.

فالاحتيال هو الاستيلاء على شئ مملوك للغير بطريقة احتيالية بقصد تملك ذلك الشيء.

والطرق الاحتيالية وفقا لنص المادة ٣٣٦ من قانون العقوبات المصري هي[١].

١ ـ الإيهام بوجود مشروع كاذب.

٢ ـ الإيهام بوجود واقعة مزورة.

٣ ـ إحداث الأمل بحصول ربح وهمي.

٤ ـ إحداث الأمل بتسديد المبلغ الذي أخذ بطريق الاحتيال.

---

(١) مصطفى مجدي هرجة: التعليق على قانون العقوبات فى ضوء الفقه والقضاء، ط ٢، ١٩٩٢، ص ١٢٧٥.

٥ ـ الإيهام بوجود سند دين غير صحيح أو سند مخالصة مزور .
٦ ـ اتخاذ اسم كاذب أو صفة غير صحيحة .
٧ ـ التصرف في مال ثابت أو منقول ليس ملكا للمتصرف ولا حق له في التصرف فيه .

وبرغم أن المشرِّع المصري قد أورد هذه الغايات على سبيل الحصر لا المثال «مما لا يتصور معه من الناحية القانونية» وقوع الاحتيال بدونها، إلا أن تلك العبارات تتسم بالمرونة وتتسع لكل الأهداف التي يسعى المحتالون إلى تحقيقها من وراء أكاذيبهم، وتهدف هذه الغايات جميعاً إلى حمل الضحية على الاعتقاد الكاذب بوجود شئ واقع أو احتمال وجوده مستقبلاً. أما الشئ الواقع فهو مشروع كاذب أو واقعة مزورة أو دين غير صحيح أو سند مخالصة مزور، أما الشئ المحتمل فهو الحصول على ربح وهمي أو تسديد المبلغ الذي أخذ منه بطريق الاحتيال .

ومن الأساليب الاحتيالية الشائعة :

أ ـ الاستعانة بشخص ثالث لتأييد الادعاء الكاذب .
ب ـ الاستعانة بأوراق ومستندات صحيحة أو كاذبة .
جـ ـ الاستعانة بوسائل الإعلام المختلفة للإعلان عن مشروع غير موجود .
د ـ التظاهر بمظاهر خادعة، كالإقامة في الفنادق الفاخرة واستخدام السيارات الفارهة والاستعانة بالحراسة الخاصة .

وكثيرا ما يتخذ محترفو تلك الجرائم من بعض الأنشطة المشروعة ستاراً لأنشطتهم غير المشروعة، وأشهر تلك الأنشطة التي قد تتخذ ستارا لتلك الجرائم هي الأنشطة التجارية، ومكاتب خدمات رجال الأعمال والتوكيلات ومكاتب الوساطة العقارية والدعاية والإعلان . . إلخ .

١ . ١ . ١ الاحتيال والتدليس المدني

برغم أن جريمة الاحتيال وفعل التدليس المدنى يشتركان في أثرهما في نفسية المجني عليه، وهو إيقاعه في الغلط، إلا أن كليهما يختلفان في أن التدليس المدني، لا يتوقف على قدر معين من الطرق الاحتيالية، وإنما يكفي مجرد الكذب، . بخلاف جريمة الاحتيال، إذ لا تقوم بمجرد الكذب، بل لا بد من توافر نوع من الطرق الاحتيالية، قدر المشرع ان الإلتجاء إليها، يمثل الحد الأدنى للخطر الاجتماعي، الذي يستوجب العقاب الجنائي[١].

ويمكن إيضاح خصائص جريمة الإحتيال على الوجه التالي[٢]:

١ ـ تنتمي إلى جرائم الأموال : لأن المشروع الإجرامي للجاني، يستهدف التوصل إلى تسلم أو نقل حيازة مال منقول مملوك للغير لنفسه أو لغيره، أو أن يتوصل إلى حمل الغير على تسليم سند ذي قيمة مالية، أو توقيع هذا السند أو إلغائه أو إتلافه أو تعديله.

٢ ـ جريمة ذات طابع ذهني، فمن أساسيات هذه الجريمة، أن تكون لدى المحتال مقدرة ذهنية على تكشف الثغرات في نظم التعامل كي ينفذ منها إلى خداع ضحاياه والقدرة على اختيار الظرف المناسب ووسيلة الخداع والتمويه التي تتناسب وشخص المجني عليه.

---

(١) أحمد فتحي سرور، الوسيط فى قانون العقوبات « القسم الخاص » ط ٣، دار النهضة العربية ١٩٨٨ ص ٢٨٨.

(٢) طاهر خليل الحبوش، جرائم الاحتيال، الأساليب والوقاية والمكافحة، من إصدارات مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض ٢٠٠١ ص ٢٢ وما بعدها.

٣ـ جريمة تقوم على تغيير الحقيقة، حيث يجب أن تقوم وسائل الخداع التي يستخدمها الجاني على الكذب، بهدف إيقاع المجني عليه في الغلط وتشويه الحقائق في ذهنه، لدفعه إلى تسليم ماله للمحتال.

٤ـ من الجرائم التي غالباً ما تستلزم التخصص والدراية من قبل الجانى بمجال نشاطه، حيث يعتاد المحتالون على استخدام أسلوب معين لارتكابها، فيتخصص به، ومن شأن هذا التخصص وتلك الدراية، أن تزيد الجاني مكراً ودهاءً وخبثاً، مما يمكنه من الإيقاع بضحاياه بسهولة ويسر.

٥ـ من الجرائم التي تنتشر في المدن والمناطق المتقدمة حضارياً، التي تزدهر بالحركة الصناعية والتجارية والاقتصادية، وعلى الأخص منها تلك التي تقوم فيها المعاملات على السرعة والائتمان.

١ . ١ . ٢ خصائص وصفات المحتال

يتميز المحتال بالعديد من الصفات دون غيره من ذوي الأنشطة الإجرامية الأخرى، فهو ذو شخصية مزدوجة حتى إنه يبدو ذا مظهر خادع عذب الكلام، يعطي وعوداً براقة، ولديه القدرة على استيعاب محيطه لمرونته في التعامل وشهامته الظاهرية. إلا أن حياته الشخصية غالباً ما تكون شديدة الاضطراب مليئة بتجارب الفشل والتخبط والأفعال اللا أخلاقية، ولا يحترم القوانين أو الأعراف أو التقاليد، ولا يشعر بالذنب تجاه الآخرين وربما يكون قد تعرض للفصل من دراسته أو من عمله أو سبق ضبطه في قضايا مختلفة وغالبا ما يميل للشهوات ويتعاطى المخدرات.

١ .١ .٣ خصائص وصفات ضحايا الاحتيال

سبق أن أوضحنا أن جانباً كبيراً من تلك الجرائم يكون للمجني عليه فيها دور بارز في تهيئة الفرصة الإجرامية للمحتال، وذلك لأسباب تتعلق بالصفات الشخصية للضحية، فضحايا هذا النوع من الجرائم غالبا ما يكونون ذوى مستوى علمي وثقافي منخفض وبعضهم ليس لديه القدر الكافي للحرص في التعامل مع الآخرين.

وهناك العديد من الضحايا الذين يتمتعون بحسن نية مفرط في التعامل مع الآخرين إلى حد التهاون في استرداد حقوقهم حياءً.

كما أن هناك العديد من الضحايا لا يتعلمون من أخطائهم، حيث يتكرر وقوعهم ضحية الاحتيال لذات الأسباب.

ثم يأتى الطمع ليكون أحد أهم الصفات التي قد تدفع صاحبها للوقوع ضحية الاحتيال من آخرين.

١ .١ .٤ إشكاليات كشف جرائم الاحتيال والإبلاغ عنها

ليس بخاف أن جانباً كبيراً من هذا النوع من الجرائم لا يتم كشفة إلا مصادفة(*)، بل إن بعضها قد لا يتم كشفه مطلقاً.

وفي جرائم بطاقات الدفع الاليكتروني ـ فإن جانباً كبيراً منها لا يتم كشفه نظرا لأن أعداداً ليست قليلة من حاملي هذا النوع من البطاقات قد اعتادوا عدم مراجعة كشوف الحسابات التي ترد إليهم من البنك.

(*) ومن الأمثلة الدالة على ذلك المحتال الذي اشهر عنه من يمكنه التدخل فى تخصيص قطع الأراضي والوحدات السكنية المميزة التي يتم توزيعها بالاقتراع نظير مبلغ من المال فكان يتقاضى نصفه مقدماً، وعند إعلان نتيجة الاقتراع يتقاضى النصف الآخر من الفائز ويقوم برد ما تقاضاه لمن لم يفز فتزداد ثقة المواطنين فيه.

كما أن جانباً كبيراً من جرائم الاحتيالات المصرفية لا يتم كشفها إلا بعد مضي فترة طويلة قد تصل إلى ستة شهور، نظراً لأن البنوك والمصارف قد اعتادت إرسال كشوف الحسابات لعملائها شهرياً أو كل ثلاثة أشهر وكل ستة أشهر حسب رغبة العميل الذي لن يمكنه كشف تلك الحالات والإبلاغ عنها قبل الاطلاع على هذا الكشف.

وكثيراً ما يحجم المجني عليهم في جرائم الاحتيال بصفة عامة عن الإبلاغ بوقوعهم ضحية الاحتيال حرصا على السمعة وخشية الحرج الاجتماعي خاصة إذا كان المجني عليه هنا من بين رجال الأعمال المعروفين.

وفي حالات أخرى يكون ضآلة المبلغ المستولى عليه سبباً في إحجام الضحايا عن الإبلاغ برغم قيام المحتال بجمع مبالغ مالية كبيرة منهم.

١ . ٢ أكثر جرائم الاحتيال انتشاراً في المجتمعات العربية

تتعدد جرائم الاحتيال في المجتمعات العربية وتتنوع أساليب ارتكابها، وضحاياها قد يكونون من الأفراد أو رجال الأعمال، كما قد يستهدف مرتكبوها شركات تجارية أو مصارف ومؤسسات مالية، وذلك على النحو التالي:

١ .٢ .١ الاحتيال على الأفراد

وقد سبق أن أوضحنا أن الأفعال المادية في هذا النوع من الجرائم تستهدف العبث بخيال الضحية، وهناك العديد من الأنماط الإجرامية في هذا المجال، منها على سبيل المثال:

١ ـ الادعاء بإمكانية تحويل أوراق سوداء عديمة القيمة إلى دولارات أمريكية باستخدام محاليل كيميائية.

٢ ـ الإعلان عن تنظيم مسابقات وهمية بغرض الاستيلاء على أموال المواطنين.

٣ ـ الاحتيال على الشباب راغبى السفر للعمل بالدول العربية والأوروبية.

٤ ـ الاحتيال على راغبي أداء فريضة الحج والاستيلاء على أموالهم.

٥ ـ إقامة دعاوى قضائية وهمية لأغراض الابتزاز.

٦ ـ الاحتيال عن طريق الرسائل القصيرة عبر الهواتف المحمولة.

ونورد هنا صوراً من تلك الأنماط[١]:

١ ـ الادعاء بإمكانية تحويل أوراق سوداء عديمة القيمة إلى دولارات أمريكية باستخدام محاليل كيميائية

انتشر هذا النوع من الاحتيال خلال السنوات الأخيرة على يد بعض العصابات النيجيرية، وانتقل بعد ذلك إلى دول غرب ووسط إفريقيا حيث احترف بعض رعاياها استهداف مواطنين من شمال أفريقيا والخليج العربي وجنوب شرق آسيا، ويتمثل هذا الأسلوب في قيام الجاني باصطياد ضحاياه عن طريق سائقي التاكسيات أو ملاك العقارات التي يؤجرونها ويقوم بإيهام الضحية بأن لديه عدة ملايين من الدولارات الأمريكية التي قام بجلبها عن طريق السفارة الأمريكية بإحدى الدول الإفريقية، وأن هذه الكمية من أوراق البنكنوت مطلية بطلاء أسود ومحفوظة داخل صندوق محكم حتى لا تتعرض للتلف أو يكتشف أمرها، وأن هذه العملات يمكن إعادتها لحالتها الأصلية بعد إزالة الطلاء الأسود الذي يعلوها باستخدام أحد المركبات

(١) من أرشيف الإدارة العامة لمباحث الأموال العامة، وزارة الداخلية، القاهرة.

الكيميائية الخاصة ويقوم بفتح الصندوق أمام الضحية وسحب ورقتين من أعلاه (هما في الأصل ورقتان صحيحتان تم طلاؤهما بمادة سوداء اللون بينما باقي محتوى الصندوق عبارة عن أوراق سوداء عديمة القيمة) ثم يقوم بإجراء تجربة أمام ضحيته لإزالة المادة السوداء من الورقتين باستخدام سائل مجهول من زجاجة صغيرة الحجم، لتظهر معالم الورقة من فئة المائة دولار أمريكي أمام الضحية، حيث يطلب منه التوجه بها لصرفها أو استبدالها من مكتب الصرافة أو البنك للعملة المحلية، فيتوجه الضحية بالورقتين ويكتشف أنها مقبولة في التداول بعد استبدالها للعملة المحلية، وعند عودته للمحتال يقوم الأخير بإيهامه بإمكان تحويل محتوى الصندوق إلى عدة ملايين من الدولارات الأمريكية الصحيحة إذا ما تم توفير كمية من السائل الكيميائي تكفي لهذا الغرض قيمتها خمسون ألف دولار أمريكي ويعقد مع الضحية اتفاقا على أن يقوم الأخير بتدبير المبلغ المشار إليه لشراء السائل الكيميائي نظير اقتسام ناتج تحويل الأوراق السوداء إلى أوراق بنكنوت صحيحة وسرعان ما تسيطر هذه الثروة الموعودة على عقل الضحية فيسعى إلى تدبير المبلغ المطلوب لشراء السائل الكيميائي وتسليمه للمحتال على أن يحتفظ لنفسه بالصندوق لحين عودة الجاني بالسائل المطلوب وهو بالطبع لن يعود.

وفي هذا الإطار تبلغ من أحد المواطنين بتقدم شخصان من الأفارقة كاميرونيا الجنسية وأخبراه أن لديهما كمية من الأوراق السوداء التي يمكن تحويلها إلى دولارات أمريكية صحيحة باستخدام مركب كيميائي، وقاما بإجراء تجربة عملية علمية أمامه على إحداهما وتحويلها إلى عملة ورقية فئة العشرين دولار قدمها المبلغ للتأكد من صحتها، وبفحصها معمليا تبين أنها عملة صحيحة.

أمكن تحديد شخصية المحتالين وتبين أنهما كانا قد قدما للبلاد للاحتيال على المواطنين بزعم تخليق دولارات أمريكية باستخدام أوراق سوداء ومواد كيميائية، ويقومان بإجراء تجربة عملية أمام الضحية ثم مغافلته وتسليمه عملات صحيحة على أنها ناتج التجربة والاستيلاء على أمواله والاختفاء.

وعقب تقنين الإجراءات وفي كمين أعد لهذا الغرض تم ضبط المذكورين أثناء قيامهما بإجراء التجربة على عملة ورقية صحيحة فئة المائة دولار أمريكي أمام الشاكي وأحد ضباط الإدارة وعثر بحوزتهما على ما يلي:

١ ـ كمية كبيرة من الأوراق السوداء بحجم الورقة فئة المائة دولار أمريكي.

٢ ـ زجاجتين بهما منظف سائل وبعض لفافات القطن.

٣ ـ ومبلغ ٤٠٠٠ دولار أمريكي، ٣٠٠٠ جنيه مصري حصيلة نشاطهما.

٤ ـ وبمواجهتهما اعترافا بنشاطهما.

٢ ـ الاحتيال عن طريق الرسائل القصيرة عبر الهواتف المحمولة

انتشر هذا الأسلوب مؤخرا بمعرفة أفراد من مصر أو لبنان أو الأردن باستهداف بعض مواطني دول الخليج الذين يتلقون اتصالات على هواتفهم المحمولة تبشرهم بالفوز بجوائز قيمة وتطالبهم بإرسال مبالغ مالية كرسوم شحن أو تأمين لاستلام تلك الجوائز.

وفي هذا الإطار كان قد تبلغ من أحد مواطني إحدى الدول العربية بتلقيه رسالة قصيرة على هاتفه المحمول بنظام SMS تضمنت أنه تم اختيار

هاتفه المحمول للحصول على جائزة مالية وطلب تحويل مبلغ ٥٥٠٠ دولار أمريكي باسم أحد الأشخاص على شركة ويسترن يونيون كرسوم قبل الحصول على الجائزة وانه قام بالفعل بتحويل المبلغ ثم اكتشف عدم صحة ما جاء بالرسالة وأنه تم الاحتيال عليه.

تم تحديد القائمين على ذلك النشاط وبضبطهم اعترفوا بنشاطهم وأنهم قاموا باختيار أرقام الهواتف بطريقة عشوائية في عدة دول عربية وتمكنوا من الاستيلاء على مبالغ مالية أخرى بالأسلوب نفسه.

١ .٢ .٢ الاحتيال على الشركات

وكثيرا ما تتعرض الشركات للاحتيال وفي أحيان أخرى قد تتخذ تلك الكيانات ستاراً لعمليات احتيالية، ومن أشهر تلك الحالات:

١ ـ إنشاء شركات مساهمة وهمية بموجب مستندات مزورة واستخدامها في الاحتيال على المواطنين «طرح أسهم للاكتتاب والتداول».

٢ ـ الادعاء بتنظيم حفلات خيرية باسم مصالح وجمعيات خيرية وهمية والاستيلاء على قيمة تذاكر تلك الحفلات من رجال الأعمال وأصحاب الشركات.

٣ ـ استغلال الشركات في الإعلان عن مسابقات وهمية بهدف جمع مبالغ مالية من المشتركين.

٤ ـ تزوير شيكات مقبولة الدفع وسجلات تجارية وبطاقات ضريبية والحصول بموجبها على بضائع من الشركات والتجار.

والحالة الأخيرة تعد الأكثر انتشارا بين أوساط الشركات، حيث يستغل المحتالون حاجة الشركات الملحة في تسويق منتجاتهم، ويتقدمون إليها

بطلبات توريد أجهزة أو سلع معمرة على أن يتم تسديد قيمة ما يتم توريده على أقساط شهرية بعد سداد مبلغ من المال على سبيل المقدم للصفقة ويتوقف المشتري عن السداد بمجرد استلام البضائع .

وفي هذا الإطار وردت للإدارة عدة بلاغات من مسئولي بعض الشركات الاستثمارية والخاصة بتعرض شركاتهم للاحتيال والاستيلاء على كميات كبيرة من السلع المعمرة والاستهلاكية بضمان شيكات بنكية مزورة ومنسوبة لإحدى الشركات الاستثمارية الكبرى .

وبعد وضع خطة بحث محكمة استهدفت تحديد القائمين على هذا النشاط ، كان أهم بنود هذه الخطة عمل نشرة سريعة للشركات الاستثمارية والتجارية التي يمكن أن تكون هدفاً لنشاط مرتكبى تلك الوقائع .

أمكن تحديد تشكيل عصابي مكون من أربعة من المحتالين «تخصص في الاحتيال على الشركات بالأسلوب التالي :

١ ـ ينتحل زعيم التشكيل صفة المدير المالي لمجموعة شركات شهيرة في مصر ، ويقوم بالاتصال هاتفياً بمديري مبيعات الشركات المستهدفة طالباً شراء كميات من الأجهزة على أن يتم تسديد القيمة بشيك بنكي منسوب لمجموعة الشركات التي ينتحل صفة مديرها المالي .

٢ ـ يقوم أحد أفراد التشكيل بالتقاط أحد سائقي سيارات النقل من الطريق العام « أو من موقفه » والاتفاق معه على نقل كمية من البضائع «بصورة طبيعية» وتكليف ذلك السائق بالتوجه للشركة المستهدفة لاستلام الأجهزة المشتراة ، بعد تسليمه مظروفا مغلقاً بداخله الشيك المزور لتسليمه في الشركة .

٣ ـ الاتصال بالسائق عقب استلامه تلك الأجهزة من مقر الشركة وتوجيهه بالحمولة إلى أحد الميادين العامة لاستلام البضاعة منه، حيث يراقبه في هذا الميدان على بعد لمراقبة مدى تتبع أجهزة الشركة له وليكون بمنأى عن الضبط.

٤ ـ ولدى اطمئنانه يقوم باستلام البضاعة ونقلها إلى سيارة نقل أخرى «سبق التقاطها من الطريق العام بمعرفة فرد آخر من أفراد التشكيل» حيث يتم تسليم تلك الأجهزة لزعيم التشكيل لتيولى بيعها بأقل من قيمتها لدى العديد من تجار الأجهزة الكهربائية بوسط المدينة.

٥ ـ نتيجة للنشرة التي تم توزيعها على الشركات ـ أبلغت احدى هذه الشركات بتلقيها اتصالا من أحد الأشخاص منتحلاً الصفة المشار إليها، فتم عمل كمين بالشركة ومراقبة السيارة التي قامت بنقل البضائع بدقة إلى أن تم نقل الحمولة إلى السيارة النقل الثانية حيث استمرت المراقبة إلى أن تم ضبط أفراد التشكيل العصابي وبحوزتهم:

أ ـ كمية كبيرة من الشيكات البنكية المزورة المنسوبة لمجموعة الشركات الشهيرة.

ب ـ عدة دفاتر شيكات بنكية منسوبة لبنوك مختلفة وبأسماء شركات مختلفة.

جـ ـ وبمواجهة أفراد التشكيل العصابى اعترف كل منهم بدوره واستيلائهم على مايلى:

ـ ١٥٠ ثلاجة من شركتي سيلتال وال جي.

ـ ١٥٠ دفاية زيت من شركة زهران.

ـ ٥٠ بوتاجاز من شركة الاتحاد الصناعي .

ـ أجهزة كومبيوتر من شركة HP .

وشروعهم في الاستيلاء على أجهزة من أربع شركات أخرى وأرشدوا عن مكان بيعهم لتلك الأجهزة .

وتبين أن زعيم التشكيل سبق ضبطه في قضايا مماثلة وتمكن من الهرب من حارسه أثناء عرضه في احدى هذه القضايا ـ حيث اتضح أنه محكوم عليه هارب من ٥٧ قضية تزوير شيكات بلغت أحكامها ٧١ عاماً .

١ . ٢ .٣ الاحتيالات المصرفية

تعيش البشرية اليوم في ظل الطفرة المذهلة التي حققتها ثورة المعلومات والاتصالات ، وكان من الطبيعى أن تعنى البنوك والمصارف بتلك الطفرة فتعاظم دورها وباتت تشارك في كافة الأنشطة الاجتماعية والاقتصادية ، وكنتيجة لتنوع الخدمات التي تؤديها زاد عملاؤها حتى أصبحت جزءاً مهماً من الكيان الاقتصادي لأية دولة .

وكان من الطبيعى أن تظهر أنماط إجرامية جديدة لم تكن معروفة من قبل ، استهدفت أموال تلك البنوك وأموال عملائها ، وارتبطت بكافة الخدمات التي يمكن أن تؤديها ، حتى إنه لا يوجد نوع من هذه الخدمات لم يكن يوما ما محلاً للاحتيال أو الشروع فيه ، منها على سبيل المثال :

١ ـ جرائم تزوير الشيكات السياحية واستعمالها .

٢ ـ جرائم تقليد الشيكات المصرفية ومقبولة الدفع .

٣ ـ جرائم أوامر الدفع والتحويلات النقدية المزورة .

٤ ـ جرائم الاحتيال في مجال الائتمان المصرفي .

٥ ـ تزوير خطابات الضمان البنكية .

٦ ـ جرائم بطاقات الدفع الاليكتروني ، التي سنتحدث عنها بشئ من التفصيل فيما بعد[١] .

وفي هذا الإطار تبلغ للإدارة من مكتب شركة الراجحى المصرفية للاستثمار بالقاهرة (مؤسسة مالية سعودية) ، بأنه قد تم اكتشاف إصدار شيكين من حساب السعودي س . ي بطريق التحايل م . س . هـ ٥٠٠ ألف دولار أمريكي وتم صرف قيمتها لمستفيدين في مصر من بنكي مصر والأهلي المصري ، وطلب اتخاذ الإجراءات القانونية في هذا الشأن .

أسفرت تحريات الإدارة على أن وراء تلك الواقعة المدعو م . س . هـ وهو من رعايا احدى الدول العربية وله إقامة بالقاهرة ، حيث كان يعمل بوظيفة محاسب لدى مؤسسة للمقاولات والتجارة يمتلكها السعودي س . ى . بجدة وأنه كان مطلعا بحكم عمله على بيانات حساب السعودي المذكور بمؤسسة الراجحى وما به من أرصدة .

وعقب حدوث خلاف بين المتحرى عنه م . س وبعض المسئولين بالشركة التي يعمل بها ، تم إنهاء عمله بها فعاد إلى القاهرة .

قام المذكور باصطناع خطابين مزورين على صورة مطبوعات شركة المقاولات ، موجهين إلى شركة الراجحي المصرفية للاستثمار بطلب إصدار شيكين مصرفيين .

---

(١) الباحث ، الاحتيالات المصرفية ، أنواعها وأساليب مكافحتها ، دراسة مقدمة للمؤتمر العربى التاسع لرؤساء المباحث والأدلة الجنائية ، تونس ١٩٩٧ ص ٩ .

الأول : بمبلغ ٣٠٠ ألف دولار أمريكي على بنك مصر الرئيسى باسم المستفيد ع . ح . ع . من حساب شركة المقاولات لدى شركة الراجحى .

والثانى : بمبلغ ٢٠٠ ألف دولار أمريكي على البنك الأهلي المصري باسم المستفيد ع . ر . ج من حساب شركة المقاولات لدى شركة الراجحي وتضمن الخطابان طلب إرسال الشيكين بالبريد السريع الدولي إلى عنوان المستفيدين بالقاهرة خصما من الحساب المشار إليه ، ثم قام بتذييل الخطابين بصورة ضوئية من توقيع صحيح للسعودي المذكور وبصمة خاتم الشركة الذى أمكنه الحصول عليها من صورة ضوئية لبعض المستندات الخاصة بالشركة التي كانت بحوزته حال عودته للقاهرة . ثم قام بإرسال الخطابين المصطنعين المشار إليهما بالفاكس إلى شركة الراجحى المصرفية للاستثمار بجدة في يومين متتاليين .

قام مسئولو الشركة بتنفيذ ما جاء بالخطابين فور ورودهما بالفاكس بعد أن تم التأكد من مطابقة التوقيعات وأن الرصيد يسمح حيث تم إرسال شيكين بالمبالغ المشار إليها بطريق البريد السريع الدولي إلى المستفيدين .

اتضح أن الخطابين المصطنعين قد تم إرسالهما بالفاكس من مركز اتصالات خدمة عامة بالقاهرة ، واتضح أن أحد المستفيدين هو صديق للمتحري عنه وأن الثانى هو حارس العقار الذي يقيم فيه بمصر الجديدة وأن الشيك الأول قد تم صرفه من بنك مصر وأن الثانى قد تعذر صرفه من البنك الأهلى المصري لارتياب الصراف في أمر حارس العقار المستفيد من الشيك .

تبين أن المتحري عنه عقب قيامة بصرف مبلغ ٣٠٠ ألف دولار أمريكي حصل لنفسه على مبلغ ٥٠ ألف دولار وقدم ٢٥٠ ألف دولار الباقية إلى البنك العربي فرع مصر الجديدة وحصل على شيك مصرفي مقبول الدفع

باسمه بذات المبلغ على بنك أمريكان اكسبريس بنيويورك وغادر البلاد في نفس يوم ورود البلاغ .

تم ضبط المستفيدين في الشيكين كما تم التحفظ على الشيك الذي تعذر صرف قيمته لدى البنك الأهلي المصري وتم إخطار البنك العربي بالواقعة ، الذي سارع بإيقاف صرف قيمة الشيك المصرفي الذي حصل عليه المتحرى عنه قبل سفره . أخطرت الشرطة الجنائية الدولية لمتابعة ضبط المتهم الهارب .

إحباط محاولة نصب دولية بالمليارات

رصدت أجهزة المكافحة بالتنسيق مع بعض الأجهزة الأمنية في مصر وصول بعض أفراد عصابة دولية للبلاد من جنسيات مختلفة وبحوزتهم شهادات ضمان بنكية مزورة لبنوك عالمية وتحمل أرقاماً فلكية بالمليارات من العملات المختلفة والذهب حيث اتضح أن كلاً من :

المدعو : D.K أمريكي الجنسية من أصل بلغاري مواليد ١٩٣٩ .

المدعوة : A.S.A بلغارية زوجة الأول

يقيمان بفندق بيراميزا بالدقي . ويدَّعى المذكور أنه ممثل لمجموعة شركات جلاكسى وهي مؤسسة مالية مقرها جاكرتا باندونيسيا وتعمل في العمليات المشبوهة بالبورصات العالمية .

أكدت التحريات احتفاظ المذكورين بغرفتهما بالفندق على كمية من الشهادات البنكية المزورة التي أحضرها للنصب بها على البنوك المصرية بغرض الحصول على قروض كبيرة بضمانها بدعوى استثمارها . . وأنهما ترددا خلال فترة تواجدهما بالبلاد على بعض البنوك لهذا الغرض بواسطة صاحب شركة سمسرة .

وبعد استئذان النيابة العامة تم ضبط المذكورين وبتفتيش حجرتهما بالفندق عثر على مايلي :

١ ـ عدد ٢٦ شهادة ضمان بنكي دولية مزورة خضراء اللون قيمة كل منها أربعة مليار و٧٩٨ مليون دولار أمريكي ومنسوبة لـ دويتش بنك .

٢ ـ عدد ٣١ شهادة ضمان بنكي دولية مزورة حمراء اللون قيمة كل منها ٢٧ مليار مارك ألماني منسوبة لـ بونذز بنك .

٣ـ عدد ١٧ شهادة ضمان بنكي دولية مزورة بيضاء اللون قيمة كل منها تسعة مليار و٤٨٠ مليون دولار أمريكي منسوبة لـ سيتى بنك .

٤ ـ عدد ٧ شهادات ضمان بنكي دولية مزورة حمراء اللون قيمة كل منها ٧٦ مليار و٧٥٠ مليون دولار أمريكي منسوبة لبنك اليابان المركزي .

٥ ـ مجموعة من قوالب الأختام الكاوتشوك والضاغطة مقلدة منسوبة للعديد من البنوك والمؤسسات المالية الدولية الكبرى واتضح أن تلك القوالب قد تم استخدامها لإصباغ الصفة الرسمية والدولية على الشهادات البنكية المضبوطة .

٦ـ كمية كبيرة من الأوراق والمستندات التي تفيد قيامهم بأعمال نصب دولية على البنوك المركزية ببعض دول العالم الثالث .

٧ـ اتضح من فحص المضبوطات أن المتهمبن ضمن عصابة دولية للنصب على البنوك، وسبق لصندوق النقد الدولي والبنك الفيدرالى الأمريكي إصدار نشرة تحذيرية من التعامل معهما .

بمواجهة المتهمين أقرا بحيازتهما لتلك الشهادات وادعيا أنها حقيقية ومضمونة من البنوك المركزية وصندوق النقد الدولي والبنك الفيدرالي الأمريكي. باشرت النيابة العامة التحقيق وأمرت بحبس المتهمين.

اتضح أن المتهمين قد عجزا عن سداد فاتورة إقامتهما بالفندق وتحررت لهما قضية أخرى في هذا الشأن.

١ .٣ الاحتيالات المالية عبر شبكة الانترنت

كان ظهور شبكة الانترنت وانتشارها، أحد أهم ثمار التزاوج الذي تم بين نظم الاتصالات وأنظمة الكومبيوتر، حيث أفضى هذا الظهور والانتشار إلى ثورة هائلة في نظم المعلومات[١].

والانترنت هي شبكة الشبكات أو الشبكة الأم التي طوت في جوفها مئات الآلاف من شبكات تبادل المعلومات، سواء كانت عالمية أو إقليمية أو محلية، وعلى الرغم من ذلك فهى كيان طفيلى، ذو مكونات مادية وغير مادية من شبكات وأجهزة وبرامج وقواعد بيانات وهى ليست ملكاً لأحد، فقد أقامت هذه الشبكة مجدها على نجاح بعض عباقرة الحاسب الآلي في وضع وتطوير بروتوكول بسيط وموحد[٢]. التزمت به جميع الشبكات

---

(١) ظهرت شبكة الإنترنت لأول مرة بمعرفة وكالة أربا ARPA التي تعمل من داخل وزارة الدفاع الأمريكية عام ١٩٦٩ تحت مسمى ARRANET ثم أتيح استخدامها للأغراض البحثية والعلمية بمعرفة بعض الجامعات الأمريكية عام ١٩٧٢، راجع نجاح محمد فوزي، جرائم المعلوماتية بين الواقع وتحديات المستقبل، كلية التدريب والتنمية أكاديمية الشرطة ٢٠٠٢ ص ٨.

(٢) وهو بروتوكول TCP/IP والذى تم تطويره واستخدامه لأول مرة عام ١٩٨٣ راجع موقع : http:// www:intenetworldstats.com

التي تريد الانضمام إلى عضوية الشبكة الأم، ضمانا لتدفق المعلومات فيما بينها، بالإضافة إلى استحداث وسائل مبتكرة من أجل سهولة التنقل ما بين مراكز خدمات المعلومات وما بين وثائقها، وانسياب مرور البيانات عبر الشبكات.

وقد ظلت شبكة الانترنت لسنوات عديدة بمنزلة المنتدى العلم للربط بين المؤسسات الأكاديمية كالجامعات ومراكز البحوث.

وقد وقف مؤسسوها الأوائل موقفاً حازماً ضد أي نشاط تجاري أو تسلل إعلاني أو إعلامي، ولم يقدر لهذه الظاهرة المعلوماتية أن تستمر، فسرعان ما أدركت القوى الاقتصادية التقليدية المزايا العديدة لهذه الشبكة، يكفينا منها قدرتها الفائقة على ربط مصادر الإنتاج بالأسواق، وكونها وسيلة فعالة لنقل بضائع صناعة الثقافة عبر طرق معلوماتها الفائقة السرعة، وكان ما كان، ووطأت مؤسسات المال والتجارة والأعلام بأقدامها الثقيلة هذا «الحرم الاكاديمي» محيلة إياه إلى متجر الكتروني وبوق اعلاني ومنافذ للتوزيع وساحة لبحوث التسويق.

ففي النصف الثانى من عقد التسعينات بدأت موجة الشركات التجارية التي ليس لها وجود سوى على شبكة الانترنت، أو ما أطلق عليها شركات الدوت كوم، حاملة معها ثورة عارمة من التطلعات ومبشرة بقفزة عملاقة للتجارة الدولية، تقود إلى ما يسمى بالاقتصاد الجديد الذي يعتمد على تكنولوجيا المعلومات ويعيش كاملاً في الفضاء الالكتروني ويتمتع بالخفة والعمل لحظياً وبالفعالية الشديدة والشفافية.

ويوضح البيان التالي تنامى أعداد مستخدمي شبكة الانترنت على مستوى العالم خلال السنوات العشر الماضية[1].

---

(١) مصدر هذه الإحصائية هو موقع http:// www internetworldstats.com/ stats.htm. وفقا لآخر تحديث بتاريخ ٣٠/ ١٢/ ٢٠٠٦.

السنة	عدد المستخدمين بالمليون
١٩٩٦	٧٠
١٩٩٧	١١٧
١٩٩٨	١٥١
١٩٩٩	٢٠٦
٢٠٠٠	٣٢٢
٢٠٠١	٥٧٤
٢٠٠٢	٦٢٥
٢٠٠٣	٧٠٠
٢٠٠٤	٨٠٠
٢٠٠٥	٩٨٠
٢٠٠٦	١٠٨٦

١ .٣ .١ الهوة الرقمية: Digital Divide

ويقصد بها تلك الفجوة الكبيرة القائمة بين المجتمعات الغنية في المجال التكنولوجى أي في المعلوماتية والاتصالات والمجتمعات الفقيرة في ذات المجال، فإذا كان العالم منقسماً إلى شمال غنى وجنوب فقير، فإن ذلك قد انعكس بدوره في عصر ثورة المعلومات والاتصالات على الدول والشركات والأفراد إلى ما يعرف بالغنى الرقمى والفقر الرقمى.

ويوضح البيان التالي توزيع حجم مستخدمى شبكة الانترنت على قارات ومناطق العالم المختلفة بالنسبة لعدد السكان.

الدولة	عدد السكان	عدد المستخدمين	النسبة المئوية
إفريقيا	٩١٥,٢١٠,٩٢٨	٣٢,٧٦٥,٧٠٠	٣,٦٪
آسيا	٣,٦٦٧,٧٧٤,٠٦٦	٣٨٧,٥٩٣,٤٥٧	١٠,٦٪
أوروبا	٨٠٧,٢٨٩,٠٢٠	٣١٢,٧٢٢,٨٩٢	٣٨,٧٪
الشرق الأوسط	١٩٠,٠٨٤,١٦١	١٩,٣٨٢,٤٠٠	١٠,٢٪
أمريكا الشمالية	٣٣١,٤٧٣,٢٧٦	٢٣٢,٠٥٧,٠٦٧	٧٠,٠٪
أمريكا اللاتينية	٥٥٣,٩٠٨,٦٣٢	٨٨,٧٧٨,٩٨٦	١٦,٠٪
استراليا والمحيط الهادي	٣٣,٩٥٦,٩٧٧	١٨,٤٣٠,٣٥٩	٥٤,٠٪[1]

(١) مصدر هذه البيان هو موقع http//www.internetworldstats.com كما يوضح ذات الموقع بياناً احصائياً لحجم مستخدمي شبكة الانترنت في دول العالم المختلفة حيث أمكن رصد مجموعة الدول العربية منه على النحو التالي :

الدولة	عدد السكان	عدد المستخدمين	النسبة المئوية
مصر	٧١,٢٣٦,٣٦١	٦,٠٠٠,٠٠٠	٩٪
الجزائر	٣٣,٠٣٣,٥٤٦	١٩٢٠٠٠٠	٥,٨٪
ليبيا	٦,١٣٥,٥٧٨	٢٠٥٠٠٠	٣,٣٪
تونس	١٠,٢٢٨,٦٠٤	٩٥٣٠٠٠	٩,٣٪
المغرب	٣٠,١٨٢,٠٣٨	٤٦٠٠٠٠٠	١٥,٢٪
جيبوتى	٧٧٩,٦٨٤	٩٠٠٠	١,٢٪
السودان	٣٥,٨٤٧,٤٠٧	٢٨٠٠٠٠٠	٧,٨٪
الصومال	١٢,٢٠٦,٢٤٢	٩٠٠٠٠	٧٪
موريتانيا	٢,٨٩٧,٧٧٨	١٤٠٠٠	٥٪
البحرين	٧٢٣,٠٣٩	١٥٢٧٠٠	٢١٪
العراق	٢٦,٦٢٨,١٨٧	٣٦٠٠٠	٠,١٪
الأردن	٥,٢٨٢,٥٥٨	٦٢٩٥٠٠	١١٪
الكويت	٢,٦٣٠,٧٧٥	٧٠٠٠٠٠	٢٦٪
لبنان	٤,٥٠٩,٦٧٨	٧٠٠٠٠	١٥,٥٪

الدولة	عدد السكان	عدد المستخدمين	النسبة المئوية
سلطنة عمان	٢,٤٢٤,٤٢٢	٢٤٥٠٠٠	١٠,١
قطر	٧٩٥,٥٠٠	١٦٥٠٠٠	٢٠,٧
السعودية	٢٣,٥٩٥,٦٣٤	٢٥٤٠٠٠٠	١٠,٨
سوريا	١٩,٠٤٦,٥٢٠	٨٠٠٠٠٠	٤,٢
الإمارات	٣,٨٧٠,٩٣٦	١٣٩٧٢٠٠	٪٣٦
اليمن	٢٠,٧٦٤,٦٣٠	٢٢٠٠٠٠	٪١,١

١ . ٣ . ٢ المخاطر والاستخدامات غير المشروعة لشبكة الانترنت

أدى اختلاف الثقافات إلى تباين واضح في الرؤي عن الأعمال التي تعد مشروعة في ثقافة مجتمع ما، بينما هي غير مشروعه في ثقافة مجتمع آخر، خاصة إذا كانت تلك الأعمال تبث من خلال آلاف المواقع ومستخدميها من مواطنى أوروبا وأمريكا الشمالية، لذا فإننا عندما نتناول الجوانب السلبية لاستخدامات تلك الشبكة ما هو مشروع منها وما هو غير مشروع، فإن تلك التفرقة سوف تكون من منطلق ثقافاتنا الشرقية بما فيها من عادات وتقاليد وقيم أخلاقية، حيث تمثل الأفعال التالية أهم الاستخدامات غير المشروعة لتلك الشبكة:

١ ـ الاقتحام غير القانونى للشبكات بغرض التسلية وتحقيق الربح.

٢ ـ الابتزاز عن طريق التهديد بتدمير شبكات الكومبيوتر والمعلومات عن طرق البريد الالكتروني.

٣ ـ السرقة أو الاحتيال.

٤ ـ غسل الأموال اليكترونياً.

٥ ـ نشر الأندية والمواقع المخلة بالآداب العامة، وكذا الصور الإباحية للأطفال.

٦ ـ الاتجار في الأعضاء البشرية.

٧ ـ استخدام الشبكة في أغراض التجسس الصناعي والتجاري.

٨ ـ احتلال المواقع.

٩ ـ الاحتيالات المالية.

١٠ ـ استخدام غرف الدردشة على الانترنت في ترويج المخدرات.

١١ ـ التهرب من الضرائب والرسوم.

ويعد خطر الاختراق عبر شبكات الانترنت أحد أهم الهواجس الرئيسية للقائمين على أمن الشبكات.

وتتعدد أسباب الاختراق فهى إما تخريبية أو بهدف سرقة معلومات ذات قيمة أو بغرض الابتزاز أو التلصص «الصناعي أو التجاري» أو مجرد إثبات الذات.

١ .٣ .٣ محترفو جرائم المعلوماتية

المجرم المعلوماتي يمثل بالنسبة للمجموعات التقليدية للإجرام، شخصية مستقلة قائمة بذاتها، فهو من جهة مثال متفرد «للمجرم الذكي» وهو من جهة أخرى «إنسان اجتماعى بطبيعته».

وتشير أبحاث علم الإجرام، إلى أنه من الناحية العلمية، فإن كل تقنية مستحدثة، ينشأ عنها في أي لحظة، وفي أي مرحلة من مراحل تطورها، الظاهرة الإجرامية الخاصة بها، وينطبق ذلك وبوجه خاص على المعلوماتية،

نظراً للإمكانات الهائلة التي تتيحها الآلة الإلكترونية، من حيث سهولة وسرعة تنفيذ الأفعال الإجرامية، وأيضا إخفاء الأدلة.

ومرتكبو هذا النوع من الجرائم هم غالباً من الشباب الذين تتراوح أعمارهم من ١٦ الى ٤٥ سنة حيث تنضم إليهم طائفة ما يسمى بصغار نوابغ المعلوماتية ويقصد بهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية، وكثيراً ما لفتوا النظر في الآونة الأخيرة عقب أفعال الإنتهاك غير المسموح بها في العديد من شبكات الحاسب الآلي[١].

١ . ٣ . ٤ قراصنة الشبكات Hackers & Crackers

محترفو الشبكات نوعان، فهما إما متلصص أطلق عليه مجازاً لفظ Hacker[٢]، أو مخرب Cracker ويعد الاختراق بنوعيه أحد أهم تداعيات هذا العصر، برغم أنه كان قد بدأ فعلياً في بدايات القرن الماضى من خلال سرقة الخطوط الهاتفية، إلا أن أول بلاغ عن جرائم احتيال باستخدام بطاقات الدفع الاليكتروني عن طريق الكومبيوتر قد وصل لجهاز مكافحة التزييف والتزوير والاحتيال الأمريكي عام ١٩٨٢م.

---

(١) محمد سامى الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة ١٩٩٨م، ص٣٩.

(٢)مصطلح Hacker أو ما يترجم خطأ بكلمة مخترق أو قرصان، بسبب فيلم أمريكي معروف حمل نفس الاسم في منتصف العقد الماضي، يدل معناه الإنجليزي «الذي ليس له مرادف دقيق فى اللغة العربية» على متخصص في نظم المعلومات والبرمجيات إلى حد الاتقان، بما يؤهله لاكتشاف أخطاء النظام العامل عليه وثغراته والعمل على تصحيحها وتلافيها، نجاح فوزي، جرائم التجارة الإلكترونية وسبل مواجهتها، دراسة مقدمة للمؤتمر الرابع لقيادات الأمن الاقتصادي بكلية التدريب والتنمية ـ أكاديمية الشرطة، ٢٠٠١م.

وقد قامت جماعة من الـ Hackers تطلق على نفسها ٢٦٠٠ في الولايات المتحدة الأمريكية بإصدار مجلة تحمل ذات الاسم في منتصف الثمانينات «ومازالت هذه المجلة تصدر ربع سنوية حتى الآن» لإتاحة كافة المعلومات وتقديم المساعدات الفنية لكل من يريد أن يتعلم ويمارس أعمال القرصنة بكافة أنواعها[١].

وفي أواخر الثمانينيات كان الاحتيال عن طريق الكومبيوتر قد انتشر على نطاق واسع، وكان من بين تلك الحالات تمكن أحد القراصنة من التسلل إلى البريد الاليكتروني لبعض الأجهزة الحكومية في الولايات المتحدة الأمريكية وقام بإتلاف أجهزة الحاسب الآلي بها.

وقد انتشرت في أوساط مواقع الانترنت في عقد التسعينيات العديد من المنظمات التي ترعى الـ Hackers أو القرصنة سعى بعضها إلى الدفاع عن المفهوم الحقيقى لهذه الجماعات الذي يتمثل في إلغاء الحدود أمام عمليات سير أغوار الحواسب والشبكات، وابتكار طرق جديدة للتعامل مع أجزائها الدقيقة والتوجه نحو التثقيف المعلوماتي، بينما حملت منظمات أخرى أهدافاً تخريبية كترويج البرامج الخبيثة ونشر طرق الاعتداء على الخصوصيات واختراق الشبكات[٢].

---

(١) قامت هذه الجماعة منذ عدة سنوات بإطلاق موقعها على شبكة الإنترنت وزاد عدد أعضائها بصورة كبيرة، حتى أصبح لها وجود مؤخرا في ١٧ دولة في مناطق متفرقة من العالم «من بينها بعض الدول العربية» وتعقد مؤتمراً شهريا يوم الجمعة الأول من كل شهر بمعرفة ممثليها في هذه الدول من الساعة ٥ م إلى الساعة ٨ م بتوقيت متزامن مع توقيت المقر الرئيسي لها في مدينة لوس انجلوس الأمريكية راجع موقع :

http:// www . 2600 . com

(٢) وكثيرا ما تلجأ الجهات الحكومية في العديد من الدول إلى التعاون مع تلك المنظمات في سبيل التوصل إلى كسر شفرة معينة أو اختراق شبكة أو موقع معين==

١ .٣ .٥ أشهر عمليات الاحتيال انتشاراً على شبكة الانترنت

ولعل أشهر عمليات الاحتيال انتشارا على شبكة الانترنت هي رسائل الاحتيال النيجيرية أو ما يسمى بـاحتيال الدفعة المقدمة Advanced Fee Fraud وقد يطلق على هذا الأسلوب أحيانا الاحتيال النيجيري ٤١٩ أو ٩ ـ ١ ـ ٤ نسبة إلى رقم المادة التي تعاقب على هذا النوع من الاحتيال في قانون العقوبات النيجيري، وقد انتشر هذا النوع من الرسائل على شبكة الانترنت في السنوات الأخيرة بشكل لافت للنظر.

ملخص الرسالة

اسم الشخص: محمد على ابن الدكتور على مصطفى مدير الحسابات في مؤسسة الذهب والمعادن الثمينة في سيراليون !! توفيت أمه منذ أسابيع ولديها ١٠ ملايين دولار في بنوك سيراليون ويحتاج لمساعدتك في إخراج هذه الأموال إلى حسابك البنكي في بلدك على أن يعطيك نسبة تصل الى ٢٠ بالمئة من المبلغ الاجمالي.

بعد أن يتصل بك عشرات المرات ويحصل على ثقتك (كونه سيأتمنك على ١٠ ملا يين دولار) سيرسل لك عشرات الوثائق الرسمية المزورة «طبعاً» ليقنعك بمصداقية الأمر، وسيطلب منك بعد ذلك بعض المبالغ

==للتوصل إلى جهات تخالف القانون، بل إن الأمور قد وصلت إلى ما هو ابعد من ذلك، حيث تقوم بعض تلك المنظمات بتنظيم مؤتمرات عالمية يجتمع فيها كل من الـ Hackers والمسئولون عن الأمن المعلوماتي وبعض عملاء من أجهزة المخابرات الحكومية للعديد من الدول في قاعة واحدة بهدف تبادل المعلومات والخبرات في أحدث ما توصل إليه العلم في مجال الأمن المعلوماتي، ومن أشهر تلك المؤتمرات مؤتمر ديفكون Defcon الذي يعقد سنويا في نهاية شهر يوليو من كل عام ومؤتمر Hope الذي تنظمه جماعة ٢٦٠٠ . .

لمصاريف المحامين وغيره، على اعتبار انه فقير وظلمته الدولة ثم سيطلب منك مبلغاً هو عبارة عن كلفة تحويل الأموال إلى حسابك البنكي. . وطبعا كل هذا كذب واحتيال وإليك التفاصيل.

قدر مكتب الخدمات السرية الأمريكية حجم المبالغ التي تم الاحتيال بواسطتها على الضحايا من جميع أنحاء العالم منذ العام ١٩٨٩م بحوالى٥ بلايين دولار أمريكي.

في استراليا في مدينة سيدنى وحدها قامت هيئة البريد الاسترالية بمصادرة ٥ , ٤ طن من الرسائل الاحتيالية النيجيرية وعليها طوابع بريدية مزورة تصل في مجموعها إلى ٨ , ١ مليون رسالة.

في يوليو ١٩٩٨م قامت الجمارك الاسترالية بتفتيش طرد مرسل بواسطة البريد السريع من نيجيريا وعثر بداخله على ٣٠٢ رسالة احتيالية كانت معدة لإرسالها بريديا من استراليا إلى عناوين في نيوزلندا، ومنطقة الباسيفيك وجنوب شرق آسيا.

في مارس ١٩٩٨م قامت شرطة هونغ كونغ باعتقال ٥٤ شخصا ومصادرة ١٣٣٥٠ رسالة احتيالية.

بدأت عصابات الاحتيال باستخدام الانترنت وقدراتها الفائقة لتوصيل رسائل الاحتيال على ملايين الضحايا باستخدام البريد الالكتروني.

وتتضمن تفاصيل هذا الاحتيال طلب مساعدة أحد الضحايا المحتملين للقيام بالمشاركة في نشاط معين تحوم حوله الشبهات، ومن ثم فإن ذلك يوفر ضمانا كافيا للمحتال بأن الضحية لن يقوم بإبلاغ أجهزة الأمن بعد وقوعه ضحية لعملية الاحتيال، كذلك فان الضحية سيكون خائفا وقلقا كونه قد ساعد في تنفيذ عملية غير قانونية ولن يعلن عن مشاركته تلك نهائيا،

وخصوصا عند احتمال وجود تغطية إعلامية لحادثة الاحتيال ونتيجة لذلك فإن المحتال سيقوم بتكرار عملية الاحتيال مرات عديدة وأحيانا مع الضحية نفسها، بينما الأجهزة الأمنية تواجه بصعوبات عديدة في العثور على الشهود والأدلة.

إن عمليات الاحتيال التي تم اكتشافها حديثا قد اتخذت العديد من الأشكال والسيناريوهات ولكنها كلها تشترك في آلية تنفيذ عملية الاحيتال حيث يتم الاتصال بالضحية بواسطة الرسائل البريدية، أو حديثا باستخدام البريد الالكتروني وذلك بدون أية اتصالات مسبقة مع الضحية، أما عناوين الضحايا فيتم الحصول عليها بوسائل عديدة : أدلة الهاتف وعناوين البريد الالكتروني، والصحف المتخصصة بالتجارة، المجلات، وغالبا ما تكون الرسائل مطبوعة أو مكتوبة بخط اليد وملصقاً عليها طوابع بريد مزورة، مما يؤدي في معظم الأحيان إلى مصادرتها من قبل مكاتب البريد.

وهذه الرسائل تشرح الحاجة إلى إخراج الأموال من نيجيريا وتطلب مساعدة (الضحية) في تزويد المحتالين بتفاصيل حسابه البنكي في بلد آخر إضافة لرسوم ومصاريف تسهيل العملية ويتم عرض نسبة عمولة على الضحية تصل إلى ٤٠٪ من المبالغ المطلوب إخراجها من نيجيريا، أما المبالغ موضوع العملية فإنها تتراوح بين ٢٠ـ ٤٠ مليون دولار أمريكي، مما يصل بالعمولة التي ستمنح للضحية إلى ١٦ مليون دولار تقريبا، وبعد ذلك يتم طلب نسبة مقدمة من الضحية يمكن أن تبلغ ٥٠٠٠٠ دولار أمريكي وهى غالبا المبلغ الذي سيتم الاحتيال به على الضحية.

تم إرسال رسائل إلى بعض الضحايا، تشير لوجود الملايين من الدولارات التي تركها أحد النبلاء أو الأغنياء لهم في وصيته ويتم دعوة

هؤلاء الضحايا للمطالبة بهذه الأموال، وإمعاناً في التضليل يتم ارفاق وصايا مزورة مع هذه الرسائل، مرسلة لأقارب الفقيد الراحل من مكاتب المحاماة وهمية، بعد ذلك يطلب من الضحية دفع مبلغ مقدم حتى يمكنهم استلام الإرث الوارد في الوصية وبالطبع فإن مثل هذا الإرث غير موجود أصلا.

الرسائل في ظاهرها صادرة عن هيئة رسمية أو شركات معروفة أو مكاتب محاماة مثل الحكومة النيجيرية، شركة البترول الوطنية، البنك المركزي النيجيري، وتوضح هذه الرسائل أن هناك مبالغ طائلة في نيجيريا ويجب نقلها إلى خارج البلاد حتى لا تتم مصادرتها، ويتم الطلب من الضحايا أن يرسلوا تفاصيل حساباتهم المصرفية لدعم عملية تحويل الأموال إلى خارج نيجيريا بصورة شرعية ومع مرور الوقت يتم الطلب من الضحايا بدفع مبالغ مقدمة لتسهيل تنفيذ عملية التحويل ومن ذلك ضرائب حكومية، رسوم حكومية، تكاليف تدقيق ومراجعة، وتأمين وحتى رشاوى للمسئولين، وغالبا ما يستمر الضحايا في دفع هذه المبالغ المقدمة لفترات طويلة على أمل الحصول على حصتهم من المبالغ الطائلة المزعومة التي لن تصلهم أبداً.

إرسال رسائل إلى بعض الضحايا حول وجود عقود حكومية مع بعض كبار المسئولين الحكوميين أو رجال الأعمال وغالبا ما تتعلق هذه العقود بشحنات للنفط الخام، أو استعادة المبالغ المتعاقد عليها أو مبالغ زائدة ناتجة عن فواتير مضخمة القيمة ولتسهيل عملية إخراج هذه الأموال من نيجيريا يتم الطلب من الضحية بأن يقوم بتزويد المحتالين بأرقام الحسابات البنكية الخاصة به ولاحقا يطلب منه دفع بعض الرسوم القانونية، مصاريف التلكس، عمولة التحويل من البنك ورشاوى للمسئولين.

ولعل المفارقة والتصعيد الأكبر يظهر في عمليات الاحتيال المتكررة ولكن على الضحية نفسها إذ إن بعض الضحايا وبعد وقوعهم ضحية لعمليات الاحتيال واكتشاف ذلك من قبلهم يقومون باستلام رسائل بعد شهور من دفعهم للمبالغ المقدمة وهذه الرسائل تظهر وكأنها صادرة من السلطات النيجيرية وتعلم الضحية فيها أن أمواله قد تم استعادتها من المحتالين وحتى يمكن إرسال هذه الأموال المستعادة للضحية فإنه يطلب من الضحية (مرة أخرى) إرسال بعض المبالغ المقدمة حتى يتسنى تحويل المبالغ المستفادة . . وهكذا يستمر مسلسل الاحتيال على نفس الضحية .

وفي وقتنا الحاضر فإن عمليات المكافحة التي تقوم بها أجهزة الأمن المختلفة قد أدت بعصابات الاحتيال إلى النزوح من نيجيريا إلى الدول المجاورة مثل جمهورية بنين، بوركينافاسو، سيراليون، غانا، الكاميرون وحتى جنوب إفريقيا، وإذا كان سبب ذلك هو الملاحقة المستمرة لأجهزة الأمن لهذه العصابات فإن شيئا آخر يتضح في عدم انتشار مثل هذا النوع من الاحتيال في هذه الدول ومن ثم تصبح إمكانية النجاح في الاحتيال أكبر بكثير .

وتوضح إحدى الرسائل الاحتيالية التي استلمها أحد الضحايا والمرسلة إليه من أحد المواطنين الزائيريين، الذى يقيم في بنين بأن هذا الزائيري يدَّعى ملكيته لحقيبتين تحتويان على عشرة ملايين دولار أمريكي والتي قام بأخذها معه عند سقوط الرئيس موبوتو، كما توضح رسالة أخرى مرسلة من أشخاص يدعون بأنهم عملاء لحركة يونيتا وبأنهم يملكون أموالا كانت مخصصة لشراء أسلحة للحركة ولكن بدلا من ذلك تم استيراد مجموعة من الماس والأحجار الكريمة بهذه الأموال، كذلك فإن استخدام البريد

الالكتروني يتيح للمحتالين إمكانية إخفاء هويتهم وإمكانية إرسال الرسالة نفسها إلى عدد ضخم من الضحايا المحتملين بسهولة كبيرة .

هل يمكن أن تتخذ بعض الاحتيالات المالية عبر شبكة الانترنت شكلاً من أشكال الجريمة المنظمة عبر الوطنية ؟

عرفت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية بأنها تلك الجريمة التي ترتكب بمعرفة جماعة إجرامية منظمة ومحددة البنية ومؤلفة من ثلاثة أشخاص أو أكثر ، موجودة لفترة من الزمن وتقوم معاً بفعل يهدف إلى ارتكاب واحد أو أكثر من الجرائم الخطيرة أو الجرائم المقررة وفقا لهذه الاتفاقية «والبروتوكولات الملحقة بها» من اجل الحصول بشكل مباشر أو غير مباشر على منفعة مالية أو منفعة مادية أخرى ويكون الجرم ذا طابع غير وطنى في حالة :

١ ـ إذا ارتكب في أكثر من دولة واحدة .

٢ ـ إذا ارتكب في دولة واحدة ولكن ضلعت في ارتكابه جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة .

٣ ـ إذا ارتكب في دولة واحدة ولكن جانب كبير من الإعداد أو التخطيط له أو التوجيه أو الإشراف عليه حدث في دولة أخرى .

٤ ـ إذا ارتكب في دولة واحدة وله آثار سلبية على دولة أخرى[١] .

وخير دليل على أن الاحتيالات المالية عبر شبكة الانترنت يمكن أن تتخذ شكلا من أشكال الجريمة المنظمة عبر الوطنية هو تحالف كاردر الدولي

---

(١) محمود شريف بسيوني ، الجريمة المنظمة وغسل الأموال في القانون الجنائي الدولي ، معهد سيراكوزا ، إيطاليا ، ٢٠٠٣م ، ص ٢٢ .

international carders Alliance حيث كان موقع Carder Planet من ابرز المواقع التي نشرت الجريمة عبر شبكة الانترنت[1].

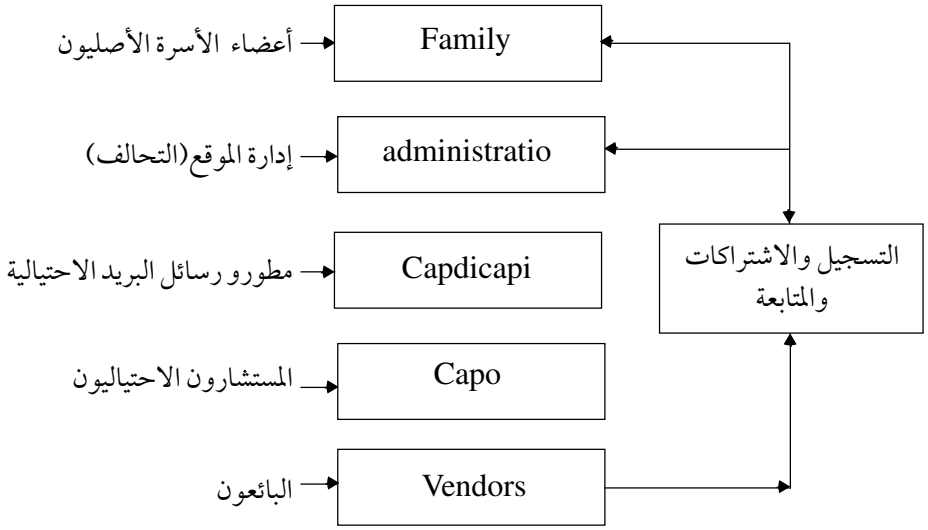
ولقد تم إنشاء وتنظيم ذلك التحالف الدولي لسرقة البيانات الخاصة ببطاقات الدفع الاليكتروني بمعرفة شخص أوكرانى الجنسية يدعى D.I.G الذي اشتهر على الشبكة بأنه الأب الروحي لنظام سرقة بيانات البطاقات عبر الشبكة وكان على قمة التسلسل الهرمي لذلك التنظيم، والذى استطاع أن يخلق سوقاً لمعلومات بطاقات الدفع الالكتروني المسروقة والتي كان يتم بيعها على الشبكة بمبالغ تتراوح بين ٤٠ إلى ٢٠٠ دولار للبطاقة الواحدة، وقد طور هذا «الأب الروحي» نشاطه الاجرامى على شبكة الانترنت بالتعاون والتنسيق مع شريكه، الاوكرانى R.V.S واللذين بدءا في تكوين خلية إجرامية كبيرة من خلال الاجتماع الذي تم عقده عام ٢٠٠١م بمدينة اوديسا بدولة أوكرانيا والذى ضم أكثر من ١٥٠ من قراصنة الانترنت من أوربا الشرقية والذى استطاعوا خلاله تبادل المعلومات والخبرات[2]، ومنذ ذلك الحين زاد حجم أعضاء تحالف كاردر الدولة International Cruder Alliance حتى وصل عدد أعضائه المشاركين إلى أكثر من سبعة آلاف عضو في جميع دول العالم «خاصة من روسيا وبعض دول جنوب شرق آسيا» حتى عام ٢٠٠٤م من خلال موقع Carder Planet والذى تم تنظيمه بشكل هرمى يضم :

---

(1)http:// forum.carderplanet.net.

(٢) تمكنت أجهزة المكافحة من ضبط R.V. S بمدينة نيقوسيا بقبرص في شهر مايو من عام ٢٠٠٣ م، بينما تم ضبط المدعو D. I. G المسمى بالأب الروحي في شهر يوليو عام ٢٠٠٥م بمعرفة الشرطة الأمريكية لمزيد من المعلومات يمكن مراجعة موقع الجهاز الأمريكي http://www.usdoj.gov / usao/press html/2004.

التركيب الهرمي لتحالف كاردر الدولي المتخصص في سرقة بيانات بطاقات الدفع الالكتروني والاتجار فيها



أعضاء الأسرة الإجرامية الأصليةFamily

إدارة المواقع Carder Planet Administration

ويرتبطون بعلاقة مباشرة مع أعضاء الـ Family ويقومون بالأعمال التجارية غير المشروعة على الشبكة ويتمتعون باحترام كبير لدى باقي أعضاء التسلسل الهرمي ومرتادي الموقع .

مطورو رسائل البريد الاحتيالية Capo DiCapi المستخدمة في سرقة بيانات البطاقة من مرتادي الشبكة .

الكابو ـ وهم لا يشتركون في أنشطة المنتدى Capo يوميا وينظر إليهم على أنهم مستشارون احتياليون

البائعون Vendors

وإذا أراد احد أن يصبح بائعاً من خلال هذا المنتدى فعليه مراجعة الأعضاء الأصليين Family ويجب على البائع أن يقوم بدفع رسوم اشتراك للأعضاء الأصليين حتى يحتفظ بموقعه وغالباً ما يكون هذا الاشتراك في حدود ١٠٠٠ دولار شهريا وخاصة للخدمة المميزة.

ونظراً لملاحقة أجهزة المكافحة في بعض الدول للقائمين على هذا المنتدى، فقد قام منظموه بإغلاقه خلال شهر أغسطس عام ٢٠٠٤ ومنذ ذلك الحين لم يتوقف المجرمون الذين كانوا يترددون على هذا المنتدى للحصول على المعلومات الخاصة بالبطاقات، بل استمروا في ممارسة نشاطهم في تلك البيئة بسرية تامة[١].

(١) شارك الباحث في ضبط العديد من الوقائع داخل مصر التى تعد من فلول هذه العناصر بالتعاون والتنسيق مع قسم مكافحة جرائم تكنولوجيا المعلومات بمنظمة الانتربول وجهاز المكافحة بإدارة التفتيش البريدي الأمريكية Us.postal Inspection service خلال عامى ٢٠٠٥م، ٢٠٠٦ م في المشروع الذي يتم تنظيمه بمعرفة المنظمة الدولية للشرطة الجنائية تحت مسمى Gold Phish.

الفصل الثاني

بطاقات الدفع الإلكتروني
النشأة، التطور، آليات العمل

٢ . بطاقات الدفع الإلكتروني: النشأة، التطور، آليات العمل

على مر الخمسمائة عام الماضية تغير أسلوب الدفع ثلاث مرات :

التغيير الأول كان من المقايضة للتعامل بالعملات المعدنية ثم التحول من العملات المعدنية إلى العملات الورقية ، ثم التحول من العملات الورقية للتعامل بالشيكات إلى أن ظهرت أخيراً بطاقات الدفع .

وتعد بطاقات الدفع الإلكتروني أو ما يطلق عليها النقود البلاستيكية بالنسبة للغالبية العظمى من الناس في مختلف أنحاء العالم شيئا إضافياً يوضع في حافظة نقودهم بجوار النقود وبطاقات إثبات الشخصية وبعض الصور ، فقليلاً ما يدركون أن هذه البطاقة الصغيرة هي أحد أهم ابتكارات هذا العصر وأكثرها تأثيراً، فقد أصبحت تلك البطاقات خلال ما يقرب من خمسين عاماً أحد أهم عناصر الحياة اليومية لملايين البشر في جميع أنحاء العالم .

وقد شكل انتشار استخدام بطاقات الدفع الإلكتروني وتنوع خدماتها محلياُ ودولياً ، دافعاً لمحترفي الاحتيال والتزوير في ممارسة أنشطتهم في التحايل والتلاعب والسرقة ، سواء من حاملي البطاقات أو التجار أو الغير ، وما يترتب على ذلك من خسائر فادحة للمصارف والعملاء .

وتعد المشاكل الناجمة عن مخاطر التعامل ببطاقات الدفع الإلكتروني من أخطر المشكلات التي تواجه الأنظمة الاقتصادية على المستويين المحلي والدولي ، خاصة بعد أن أظهرت الإحصاءات تزايد حجم الخسائر الناجمة عن التلاعب والتحايل ببطاقات الدفع وهو ما دفع المؤسسات والهيئات الدولية المسئولة عن إصدار هذا النوع من البطاقات إلى اتخاذ العديد من

التدابير الفنية والمصرفية لمواجهة هذا الخطر واتجهت العديد من الدول إلى سن التشريعات اللازمة لردع مرتكبي هذا النوع من الجرائم.

ولكن كيف ومتى بدأ عالم بطاقات الدفع الإلكتروني؟ وما هي أنواعها ومزاياها؟ وكيف تطورت وأثرت وتأثرت بالتقدم العلمي والتكنولوجي ؟

هذا ما سنحاول الإجابة عليه وذلك من خلال ثلاثة مباحث :

ففي المبحث الأول نتحدث عن هذا النوع من البطاقات من حيث النشأة والتطور والمزايا والأنواع، بينما نتحدث في المبحث الثاني عن تطور العمليات المصرفية الاليكترونية وأثره في تطبيقات بطاقات الدفع أما في المبحث الثالث فنتحدث عن صور وحدود العلاقة بين البنك والتاجر.

٢ .١ بطاقات الدفع الإلكتروني: النشأة والتطور

في أحد أيام عام ١٩٤٩ حصل السيد فرانك ماكنمارا «أحد رجال البنوك الأمريكية» على فاتورة لتسديد قيمة غذاء عمل، كانت قيمة الفاتورة باهظة إلى الحد الذي اضطره للاتصال بزوجته لتحضر له نقوداً من المنزل ليستطيع تسديد قيمة فاتورة المطعم، ولتجنب الوقوع في مثل هذا الموقف الحرج مرة أخرى جاء هذا الرجل بفكرة بطاقة الدفع، فأنشأ مؤسسة داينرز كلوب Diners Club بمساعدة اثنين من رجال البنوك المتخصصين في عمليات التجزئة المصرفية وهما بلومنج داليز، شنايدر[1] Blooming Dales & Sneider وأصدرت تلك المؤسسة أول بطاقة دفع عام ١٩٥٠م لعدد ٢٠٠ عضو وكانت تلك البطاقة مقبولة لدى ٢٧ مطعماً، وسرعان ما لاقت تلك الفكرة القبول لدى المواطنين فأقبلوا عليها، حتى بلغ عدد حاملي تلك البطاقة

(١) راجع «مجتمع اللا نقود» كتيب تعريفي من إصدارات منظمة الفيزا العالمية القاهرة ٢٠٠٦م، Visa Egypt، ص٣٠.

عشرين ألفاً بنهاية العام، يتمتعون بما تتيحه العديد من الفنادق والمطاعم داخل ولاية نيويورك[1].

وفي عام ١٩٥٨م قامت شركة أميركان إكسبريس American Express وهي شركة أمريكية تعمل في «مجال الخدمات المالية والسياحة والسفر» بإصدار بطاقة دفع خاصة بعملائها وتلاها في العام نفسه قيام بنك أوف أميركا Bank of America بإصدار بطاقة ائتمان سميت بطاقة أمريكارد Americard.

وفي عام ١٩٦٦م كان هناك ١٤ بنكاً أمريكياً لديه الصلاحية في إصدار بطاقة بنك أمريكارد ـ Americard ـ. وفي العام نفسه تأسست مؤسسة مالية جديدة تحت مسمى انتر بنك كارد -Interbank Card Association- التي قامت بإصدار بطاقة دفع ماستر Master Charge.

وفي عام ١٩٦٧م قامت مؤسسة دي لارو -De La Rue- بإنتاج أول ماكينة صرف نقود آلية -ATM-[2] لبنك باركليز الإنجليزي.

وفي عام ١٩٧٢م ظهرت أول ماكينة صرف نقود آلية وATM «تعمل من خلال شبكات الاتصالات Online» باستخدام البطاقات البلاستيكية ذات الشريط الممغنط.

---

(١) راجع :http:// www.papacs.org.uln
ويعود تاريخ ظهور أول بطاقة في الحقيقة إلى مؤسسة وسترن يونيون Western Union عام ١٩١٤م وهي مؤسسة مالية أمريكية تعمل في تحويل الأموال، التي أصدرت بطاقات معدنية ـ Metal Cards، لعملائها المميزين، التي أطلق عليها بعد ذلك النقود المعدنية ـ Metal Money ـ، وفي عام ١٩٢٤م قامت شركة الولايات المتحدة العامة للبترول في كاليفورنيا التي أصبحت فيما بعد شركة موبيل أويل Mobil Oil بإصدار بطاقة معدنية لموظفيها وعملائها لاستخدامها لدى محطات الخدمة الخاصة بها فقط راجع أيضاً http://www.westernunion.com/history.

(٢) ATM هي اختصار لـ Automated Teller Machines

وفي عام ١٩٧٣ م شهدت صناعة بطاقات الدفع الإلكترونية طفرة كبيرة حين قامت مؤسسة أمريكارد التي أصبحت مؤسسة فيزا العالمية VISA International فيما بعد بتأسيس أول نظام إليكتروني لتشغيل بطاقات الدفع، وأدى هذا النظام فور ابتكاره إلى تقليل الوقت اللازم لإجراء معاملة البطاقة من خمس دقائق إلى ٥٦ ثانية، بالإضافة إلى خفض معدلات السرقة والاحتيال، وخلال العام التالي استطاع البنك بفضل هذا النظام الإلكتروني الجديد توفير ٣٠ مليون دولار أمريكي وكان Jcpenny هو أول متجر داخل الولايات المتحدة يقبل التعامل ببطاقات الدفع[١]، وأدت زيادة المبيعات التي حققها هذا المتجر إلى تشجيع العديد من المحلات التجارية الأخرى وإقبالها على التعامل بالبطاقات.

وفي عام ١٩٧٦م تحول بنك أمريكارد Bank Americard إلى مؤسسة فيزا الدولية VISA International وصدرت أول بطاقة تحمل شعار فيزا VISA.

وفي عام ١٩٧٩ م بطاقة دفع ماستر Master Charge أصبحت ماستركارد Master Card.

وفي عام ١٩٨٤ م سعت مؤسسات الدفع لتحقيق القبول العالمي لبطاقات الدفع عن طريق توسيع شبكة بنوكها وتجارها في جميع أنحاء العالم عن طريق تأسيس ونشر نقاط قبول بطاقات الدفع في قارات العالم السبع، وأدت هذه الخطوة إلى ميلاد جيل جديد من البطاقات المختلفة مثل بطاقة المكافآت وبطاقة الخصم، وبطاقة ماكينة الصرف الآلي خلال الثمانينيات والتسعينيات من القرن نفسه.

---

(١) راجع «مجتمع اللا نقود» كتيب تعريفي من إصدارات مكتبة منظمة الفيزا العالمية بالقاهرة ٢٠٠٦م، ص ٣٠.

٢ . ١ . ١ توصيف بطاقات الدفع الإلكتروني

بطاقة الدفع الإلكتروني من ناحية الشكل، هي قطعة من البلاستيك لها مواصفات كيميائية محددة Polly venile clorid PVC ذات أبعاد قياسية هي «طول ٦ , ٨٥مم × عرض ٩ , ٣٥مم» ويبلغ سمكها ٧٦ , ٠مم[١]. مدون عليها بيانات مرئية وملقنة ببيانات أخرى غير مرئية، ويقترن إصدار البطاقة لحاملها بمنحه رقماً سرياً يعمل حال استخدام البطاقة في وسط إليكتروني والتوقيع عليها بتوقيعه، وتصدر عن بنوك أو منظمات ذات ثقة تضمن تعاملات العميل في شبكة التعامل بالبطاقة، وبموجبها يمكن الشراء والدفع وسحب الأموال والحصول على الخدمات[٢].

أما مصرفياً، فهي أداة للوفاء بالالتزامات، مقبولة على نطاق واسع محلياً ودولياً لدى الأفراد والتجار والبنوك كبديل للنقود لدفع قيمة السلع والخدمات المقدمة لحامل البطاقة مقابل توقيعه للتاجر على إيصال بقيمة التزامه الناشئ عن شرائه سلعة أو حصوله على خدمة، على أن يقوم التاجر بتحصيل قيمة الإيصال من البنك المصدر للبطاقة عن طريق البنك الذي صرح له بقبول البطاقة كوسيلة دفع، ويطلق على عملية التسوية بين البنوك الأطراف فيها اسم نظام الدفع الإلكتروني والذي تقوم بتنفيذه الهيئات الدولية المصدرة للبطاقات[٣].

---

(١) ISO 7816-1 راجع موقع منظمة الأيزو العالمية http://www.iso.org

(٢) رياض فتح الله بصلة، جرائم بطاقات الائتمان، القاهرة، دار الشروق ١٩٩٥م، ص ٧٩.

(٣) عطية سالم عطية التعريف بنظام بطاقات الدفع الإليكتروني، دراسة مقدمة لندوة الصور المستخدمة لجرائم بطاقات الدفع الإليكتروني، مركز بحوث الشرطة، أكاديمية الشرطة، القاهرة نوفمبر ١٩٩٨ م، ص ٧.

٢ .١ .٢ أطراف العملية التجارية

وتعد بطاقات الدفع الإلكتروني وسيلة مفضلة لدى المستهلكين حيث أنها تسهل لهم عمليات الشراء اليومية في أي وقت وأي مكان دون الحاجة لحمل مبالغ كبيرة من النقود، كما أنها توفر لهم الراحة والمرونة والأمان وتسمح لهم بممارسة الحياة بأسلوب أكثر سهولة، ولكن هذا لا يعني أن نظم تشغيل وإصدار هذه البطاقات بسيطة وسهلة، حيث تشمل كل معاملة على أربعة أطراف وهم:

- المستهلك« حامل البطاقة».
- البنك مصدر البطاقة.
- التاجر.
- البنك الذي يتولى التحصيل للتاجر.

١ ـ المستهلك أو حامل البطاقة

وهو الشخص الذي يحصل على بطاقة دفع من البنك المصدر لاستخدامه الشخصي لها كوسيلة دفع مقابل الحصول على السلع والخدمات ودفع تكاليف السفر والسياحة وإتمام الصفقات التجارية الصغيرة والحصول على احتياجاته النقدية من البنوك المصرح لها بالتعامل وفق هذا النظام أو من خلال آلات الصرف الآلي ATM في كافة أنحاء العالم بدلاً من أخطار حمل النقود.

ويحصل المستهلك على البطاقة عن طريق تعاقده مع البنك المصدر لها، بتوقيعه على طلب الحصول عليها، والذي يتضمن شروط استعمالها، حيث يعد توقيع العميل على هذا الطلب بمثابة موافقة منه على إصدار البطاقة وأن

استعماله لها محكوم بالشروط الواردة في الطلب، ولا يقوم البنك بإصدارها إلا بعد دراسة طلب العميل جيداً وبعد التأكد من وجود الضمانات الكافية «عينية أو شخصية» والتي تتناسب مع السقف الائتماني «حد الاستخدام» المصرح للبطاقة.

٢ ـ بنك العميل حامل البطاقة Issuer Bank

هو البنك الذي له حق إصدار بطاقات الدفع الإلكتروني لعملائه ولا يكون للبنك الحق في ذلك إلا بعد الحصول على موافقة الهيئة الدولية «سواء كانت VISA MasterCard» على التعامل بهذا النظام، ولا تعطى هذه الهيئات الموافقة إلا للبنوك أو المؤسسات المالية الكبيرة ذات المقدرة المالية والفنية على استخدام النظام، ويكون لكل بنك رقم خاص به يتم من خلاله التعامل مع البنوك الأعضاء بالهيئة الدولية، ويكون هذا الرقم من الثمانية أرقام الأولى من اليسار المطبوعة على البطاقات المصدرة من هذا البنك.

٣ ـ منافذ البيع أو التجار Merchants

وهي التي تقبل البطاقات من حامليها كوسيلة دفع إلكترونية لقيمة السلع والخدمات المقدمة منها لهؤلاء العملاء مقابل توقيعهم للتاجر على إيصالات وإشعارات المبيعات «بقيمة التزامهم الناشئ عن شرائهم للسلع أو الحصول على الخدمات من هذا التاجر، ولا يحق لأي تاجر أو جهة ما قبول تلك البطاقات «من حامليها كوسيلة دفع» دون وجود تعاقد مع أحد البنوك العاملة وفق هذا النظام، والذي يقوم بتزويد التاجر بالأجهزة أو الأدوات اللازمة للتعامل في هذا النشاط «سواء كانت إلكترونية أو يدوية»لمستلزمات التشغيل الخاصة بها «إشعارات المبيعات على أن يقوم التاجر بتحصيل قيمة تلك الإشعارات من البنك المتعاقد معه.

وتشمل الجهات التي تقبل التعامل ببطاقات الدفع الإلكتروني جميع أوجه النشاط التجاري والاقتصادي، المحال التجارية، الفنادق شركات الطيران، شركات السياحة، المطاعم، البازارات، مكاتب تأجير السيارات. . . . الخ.

٤ ـ بنك التاجر Acquirer Bank

وهو البنك الذي يقوم بالتعاقد مع التجار لتقديم خدمة تحصيل إشعارات المبيعات لهم مقابل عمولة معينة يتفق عليها بين البنك والتاجر، ويقوم البنك بتزويد التجار المتعاقدين معه بالأجهزة ومواد الدعاية ومستلزمات التشغيل اللازمة لاشتراك التاجر في هذه المنظومة وهي إما يدوية أو إلكترونية (POS- Point of Sale).

ويقوم التاجر بالتوقيع على العقد «اتفاقية التاجر» والذي بناء عليه يوافق التاجر على قبول البطاقات البلاستيكية كوسيلة دفع إلكترونية دولية وفقاً للشروط والأوضاع التي يحددها البنك والمدونة في العقد.

وبرغم أن أطراف العملية هم الأربعة السابق ذكرهم، إلا أن للهيئات الدولية المنظمة لهذا النشاط (مثل فيزا VISA وماستركارد Master Card) الدور الأساسي والأهم، فهي التي تصرح للبنوك والمؤسسات المالية في جميع أنحاء العالم بالتعامل وفق هذا النظام، سواء بإصدار البطاقات للعملاء، أو تحصيل قيمة إشعارات المبيعات للتجار، ويتم عن طريقها عمليات المقاصة والتسويات الإلكترونية وتحويل الأموال من بنك العميل حامل البطاقة وبنك التاجر «القائم بعملية التحصيل».

٢ .١ .٣ أهم المنظمات والمؤسسات المالية الدولية العاملة في مجال البطاقات

١ ـ مؤسسة فيزا الدولية VISA International Service Association

ومقرها الرئيس الولايات المتحدة الأمريكية ـ لوس أنجلوس .

لا تصدر أي نوع من البطاقات ولكنها تعطى عضويتها لبنوك تتولى إصدار البطاقات والتعاقد مع التجار وتمارس نشاطها في جميع أنحاء العالم من خلال ست مناطق رئيسة .

أ ـ اليابان وآسيا والمحيط الهادي .

ب ـ كندا .

جـ ـ غرب ووسط أوروبا .

د ـ شرق أوروبا والشرق الأوسط وإفريقيا .

هـ ـ أمريكا اللاتينية .

و ـ الولايات المتحدة الأمريكية .

٢ـ مؤسسة ماستركارد العالمية Master Card International

ومقرها الرئيسي بالولايات المتحدة الأمريكية ـ سانت لويس ، نيويورك .

لا تصدر أي نوع من البطاقات ، ولكنها تمنح عضويتها لبنوك تتولى إصدار البطاقات والتعاقد مع التجار ، وتمارس نشاطها في جميع أنحاء العالم من خلال ٦ مناطق رئيسية أيضاً مثل منظمة فيزا «تقريباً» .

٣ ـ شركة أميركان إكسبريس American Express

مقرها الرئيسي الولايات المتحدة الأمريكية . وتقوم بإصدار بطاقاتها والتعاقد مع التجار مباشرة من خلال فروعها المنتشرة في جميع أنحاء العالم ولا تعطي عضويتها لبنوك أو مؤسسات مالية أخرى .

٤ ـ مؤسسة داينرز كلوب الدولية Diners Club International

ومقرها الرئيسي الولايات المتحدة الأمريكية وهي تمنح عضويتها لبنوك مؤسسات مالية لتتولى إصدار البطاقات والتعاقد مع التجار .

٥ ـ مؤسسة JCB

ومقرها الرئيسي اليابان وأعضاؤها من البنوك اليابانية .

٢ . ١ . ٤ دور المنظمات والهيئات الدولية في نشاط بطاقات الدفع الإلكتروني

تضطلع الهيئات والمنظمات الدولية مثل فيزا VISA ، ماستر كارد Master Card بدور مهم في هذه المنظومة يتمثل في[١] :

١ ـ تضفي هذه الهيئات القبول والصفة الدولية للبطاقات المصدرة من البنوك الأعضاء المصرح لهم بالتعامل في هذا المجال .

٢ ـ تقوم بإدارة عمليات بطاقات الدفع الإلكتروني من خلال شبكات المعلومات والاتصالات الخاصة بها ، والتي توفر للبنوك الأعضاء عمليات المقاصة والتسويات الإلكترونية فيما بينهم .

٣ـ وضع المعايير والنظم وتحديد القواعد والإجراءات التي تقوم البنوك الأعضاء بتطبيقها ، لتحديد حقوق والتزامات كل عضو ومدى مسئوليته تجاه الآخرين .

---

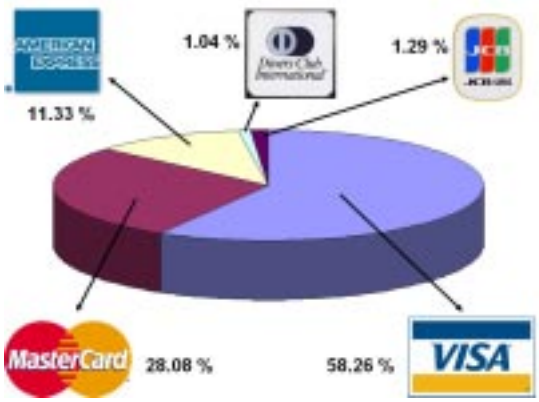
(١) عطية سالم عطية ، مرجع سابق .

٤ ـ تقوم بدور لجنة التحكيم في حالة النزاعات بين أعضائها .

وقد بلغ حجم البطاقات بنوعيها « إئتمان وخصم » على مستوى العالم حتى نهاية عام ٢٠٠٥م ١,٧٧ مليار بطاقة .

وتستحوذ منظمة الفيزا العالمية على النصيب الأكبر من حجم البطاقات المصدرة على مستوى العالم بنسبة ٥٨,٢٦٪ بينما تأتي منظمة ماستر كارد في المرتبة الثانية بنسبة ٢٨,٠٨٪ ثم أميريكان إكسبريس بنسبة ١١,٣٣٪ و JCB بنسبة ١,٢٩٪ وداينرز كلوب بنسبة ١,٠٤٪ فقط[١] .

بيان يوضح توزيع حجم البطاقات بين المؤسسات المالية الدولية على مستوى العالم



(١)راجع تقرير نيلسون على موقع http://www.nilsonreport.com وهى شركة متخصصة فى بحوث السوق الخاصة بنظم الدفع الإليكترونية، مع ملاحظة أن إحصائيات عام ٢٠٠٦م لم تكن قد تم إعدادها بعد .

وتضم منظمة الفيزا في عضويتها ٢١,٠٠٠ واحداً وعشرين ألف بنك ومؤسسة مالية تمارس نشاطها من خلال ٢٤ مليون تاجر ومنشأة.

٢ .١ .٥ أركان البطاقة[١]

سبق أن أوضحنا أن جميع أنواع البطاقات تتشابه في بنائها المادي من كونها مصنوعة من البلاستيك وذات أبعاد قياسية محددة (٦,٨٥مم× ٩,٥٣مم)، إلا أنها تختلف عن بعضها في نوعية المعادلة التي تقوم بها، وفي نوعية العلاقة بين حامل البطاقة والبنك المصدر لها، وعلى الرغم من ذلك فإن أركان البطاقات الأساسية لا تتغير وهي:

١ ـ رقم البطاقة: وهو الرقم المطبوع على البطاقة والمسجل بملفات البنك المصدر لها وهو مكون من ستة عشر رقماً أو ثلاثة عشر.

٢ ـ اسم حامل البطاقة: وهو اسم طالبها الذي يقوم بالتوقيع على البطاقة والمصرح له باستخدامها.

٣ ـ تاريخ الإصدار: وهو الشهر الذي أصدرت فيه البطاقة ويبدأ سريانها من تاريخ إصدارها.

٤ ـ تاريخ الصلاحية: وهو الشهر الذي تنتهي فيه صلاحية البطاقة ولا يجوز لحاملها استخدامها بعد ذلك التاريخ، كما لا يجوز للتجار قبول التعامل بها بعده، إذ تصبح البطاقة غير سارية.

٥ ـ اسم البنك المصدر: وهو البنك المصرح له من قبل الهيئات الدولية بإصدار البطاقات ويظهر رقمه المحدد من قبل الهيئات الدولية واسمه وشعاره على البطاقات التي يصدرها.

---

(١) عطية سالم عطية، مرجع سابق.

٦ ـ شعار الهيئة الدولية : وهو القاسم المشترك على جميع البطاقات المصدرة بتصريح من تلك الهيئة بصرف النظر عن البنك المصدر والذي يعطيها القبول والانتشار الدولي .

٧ ـ حد السحب«أو الاستخدام» [لا يظهر] وهو الحد المقرر للبطاقة والذي يقرره البنك المصدر لها وفقاً للقواعد والنظم التي يقررها ، ويقوم العميل باستخدام بطاقته في حدود الحد المقرر لها سلفاً من البنك المصدر لها ، والمدون بحساب بطاقة العميل على الحاسب الآلي بالبنك .

٨ ـ الشريط الممغنط : هو المكان المخصص على البطاقة لتخزين البيانات الإلكترونية الخاصة ، والتي يتم قراءتها عند استخدام البطاقة في نقاط البيع الإلكترونية POS وآلات الصرف الآلي ATMs ويتم نقل البيانات الملقنة للشريط الممغنط إلى البنك المصدر للتأكد من صحة بياناتها وأخذ الموافقة على الصرف بعد التأكد من كفاية رصيد البطاقة .

٩ ـ الصورة المجسمة ثلاثية الأبعاد : (هولوجرام) Hologram وهي العلامة المميزة للهيئة الدولية والتي تظهر بجوار شعارها وهي تماثل العلامة المائية في النقود الورقية ، ومن خلالها يمكن التحقق من سلامة البطاقة .

١٠ ـ شريط التوقيع : وهو المكان المخصص لتوقيع حامل البطاقة ، ويقوم التاجر أو الصراف بمطابقته مع توقيع حامل البطاقة على إشعار المبيعات أو الصرف .

١١ ـ رقم التمييز الشخصيPin [لا يظهر]: أو ما يطلق عليه الرقم السري وهو مكون من ٤ أرقام، يسلم للعميل بمظروف مغلق عند استلامه للبطاقة(*) ويستخدمه حامل البطاقة عند الصرف النقدي من ماكينات الصرف الآلي ATM، والذي من خلاله تتعرف الماكينة على صاحب البطاقة وتسمح له بالصرف في حالة إدخاله للرقم السري الصحيح.

توصيف لمكونات بطاقات ماستر كارد من الوجهين

توصيف لمكونات بطاقات فيزا من الوجهين

(*) تطورت عملية تحديد رقم التميز الشخصيى « Pin» مؤخرا حيث اتجهت العديد من البنوك الى تمكين العميل من اختيار الرقم السري الخاص به، وذلك بتخليقه من خلال ماكينة إليكترونية مرتبطة بشبكة معلومات البنك وبعيدا عن أعين موظفيه، راجع موقع http://www.citybank.com.

٢ .١ .٦ أنواع بطاقات الدفع الإلكتروني «مصرفياً»

تخضع بطاقات الدفع لأحد نظامين متميزين وهما الائتمان والخصم .

١ ـ بطاقة الائتمان Credit Card

وتعمل بطاقة الائتمان طبقاً لنظام القرض المحمول، فعندما يصدر البنك بطاقة ائتمان لأحد الأشخاص، فإنه يحدد له سقفاً ائتمانياً معيناً، أو حد أقصى للنقود التي يمكن أن ينفقها باستخدام البطاقة، ويقوم البنك بتحديد السقف الائتماني لكل عميل وفقاً للضوابط الموضوعة سلفاً. وفور حصول العميل على تلك البطاقة فإنه يمكنه استخدامها في الشراء لدى المحال التجارية أو الحصول على الخدمات بدلاً من الدفع النقدي، وتلك المعاملات يتم تسجيلها فور حدوثها ويقوم البنك المصدر للبطاقة بالتسديد فوراً، كما يمنح العميل فترة سماح تراوح بين ٣٠, ٥٥ يوماً يمكنه السداد خلالها .

وفي نهاية كل شهر يرسل البنك للعميل كشف حساب يتضمن كل المعاملات التي استخدمت فيها البطاقة، ليتولى العميل تسديد إجمالي القيمة المستحقة عليه خلال فترة السماح، أو تسديد جزء من إجمالي المبلغ المستحق يمثل نسبة ٥٪ إلى ١٠٪ كحد أدني حسب قواعد كل بنك عندئذ يقوم البنك

باحتساب نسبة فائدة على المبلغ المتبقي الذي لم يتم تسديده وبنفس القواعد المطبقة على فوائد القروض[١].

٢ ـ بطاقة الخصم Debit Card

تشكل بطاقة الخصم الجزء الأكبر من حجم بطاقات الدفع المصدرة حول العالم، حيث نجد أن ربع عدد سكان العالم البالغين يستخدمونها[٢]، فهي توفر لهم الراحة والأمان.

إن بطاقات الخصم تماثل بطاقات الائتمان من حيث الشكل، فكلتاهما بطاقات بلاستيكية تحمل اسم صاحبها ورقم حسابه ويتم استخدامها لسداد المدفوعات، ويتضح الفرق بين البطاقتين من حيث الاسم، فكلمة ائتمان تعني اقتراض وكلمة خصم تعني سحب من رصيد فعلي. وهكذا نجد أن بطاقة الائتمان تتيح لصاحبها السداد فيما بعد، بينما توجب بطاقة الخصم الدفع الفوري متزامناً مع حدوث المعاملة، لذا فإن بطاقة الخصم تكون مرتبطة مباشرة بالحساب البنكي لصاحبها، أي أنه عندما يقوم العميل باستخدامها فإنه يستخدم رصيد حسابه البنكي فقط[٣].

---

(١) بعض البنوك تطلب قيام العميل بفتح حساب لديها مقابل حصوله على تلك البطاقة، والبعض الآخر يطلب من العميل إيداع مبلغ من المال كوديعة. بالإضافة إلى ذلك تقوم البنوك بفرض رسوم سنوية مقابل الخدمات التي تؤديها وكذا رسوم ضئيلة على معاملات السحب النقدي من ماكينات الصرف الآلي ATMs التي تتم باستخدام بطاقة الائتمان. وتختلف نسبة الفوائد ورسوم الخدمات من بنك لآخر.

(٢) راجع موقع منظمة الفيزا العالمية على شبكة الإنترنت http://www.visa.com

(٣) أضاف البعض «ممن تناولوا هذا الموضوع بالدراسة» أنواعا أخرى من البطاقات مثل بطاقة الدفع المؤجل Charge Card وهي بطاقة غير منتشرة وكذا بطاقة الصراف الآلي ATM Card وهي تدخل في عداد بطاقات الخصم، وأيضاً بطاقة ضمان الشيكات مثل بطاقة Euro Card والتي تضمن تعاملات Euro Cheque وهي تعد أيضاً من بطاقات الخصم لارتباطها برصيد صاحبها. راجع الباحث الاحتيالات المصرفية ـ أنواعها وأساليب مكافحتها مرجع سابق.

٢ . ٢ تطـــور العمليـــات المصرفيـــة الإلكترونيـــة وأثـره في تطبيقات بطاقات الدفع

كان من الطبيعي أن يترك التطور التكنولوجي أثره الواضح في نظم المدفوعات بشكل عام ، وقد بدأ ذلك جليا في ظل التطور الذي لحق بكل من نظم المعلومات وأنظمة الاتصالات والاندماج الذي تم بينهما فظهرت تكنولوجيا الدوائر المتكاملة Integrated circuits التي تم استخدامها فيما بعد في البطاقات الذكية أو الرقائقية .

ومع ظهور شبكة الإنترنت وتنامي استخداماتها بدأت في النصف الثاني من عقد التسعينيات موجة الشركات التجارية التي ليس لها وجود سوى على شبكة الإنترنت ، أو ما أطلق عليها شركات الدوت كوم ، حاملة معها ثورة عارمة من التطلعات ومبشرة بقفزة عملاقة للتجارة الدولية ، تقود إلى ما يسمى بالتجارة الإلكترونية ، التي تعتمد على تكنولوجيا المعلومات وتعيش بصورة كاملة في الفضاء الإلكتروني .

كما شهدت العمليات المصرفية تطوراً ملحوظاً تمثل في تمكين عملاء البنوك من إجراء معاملاتهم المصرفية من خلال مواقع تلك البنوك على شبكة الانترنت ، فيما سمى بالعمليات المصرفية الاليكترونية ، واتيحت فرصة التحويلات النقدية التي ارتبط بعضها مع بطاقات الدفع الاليكترونى من خلال تلك الشبكة

ونستعرض فيما يلى كلاً من :

ـ البطاقات الذكية كأحد أهم الحلول التكنولوجية الحديثة لتأمين تعاملات بطاقات الدفع الإليكتروني .

ـ التجارة الاليكترونية كأحد أهم تطبيقات استخدامات بطاقات الدفع الاليكترونى.

ـ التحويلات المصرفية عبر شبكة الانترنت «والتي بدأت تنتشر في العديد من بلدان العالم» باستخدام بطاقات الدفع الاليكترونى

أولاً: البطاقات الذكية أو البطاقات الرقائقية Smart Cards or Chip Cards

وقد يطلق عليها البطاقة ذات الدوائر المتكاملة Integrated Circuts هى بطاقة بلاستيكية بذات أبعاد ومواصفات البطاقة الممغنطة، إلا أنها تحتوي على شريحة من الدوائر المتكاملة مدمجة بها، تعمل كذاكرة إلكترونية ذات سعات تخزينية مختلفة، تستخدم في العديد من التطبيقات، وتعد التطبيقات المصرفية أحد أهم استخدامات هذا النوع من البطاقات.

تم ابتكار وتسجيل هذا النوع من الشرائح الذكية عام ١٩٧٤م على يد الفرنسى ولاندمورينو[١]، وفي عام ١٩٧٧م قامت ثلاث شركات كبرى هى هانى ويل بل، Honewell Bull، فيليبس Philips، شلامبرجيه Shlumberger، باستثمار رأسمال ضخم لتطوير هذه التكنولوجيا، وكان أول استخدام لها عام ١٩٨٣م عندما قامت شركة الاتصالات الفرنسية

(١) راجع Http://en.wikipedia.oirg/wikilchip-card
راجع أيضاً Andrew sclark paper on http://www.primarykey.co.uk

PTT بقبولها في محاسبة التليفونات العامة. حيث حلت «البطاقة التي تحمل شرائح ذكية» مشاكل التزييف والتأمين التي كانت تواجه عملية جمع العملات من كبائن المواقف، وقد واصل تطور البطاقات الذكية حتى تم استخدامها في بعض البنوك الفرنسية عام ١٩٨٤م.

وكانت النقلة الثانية في تطور استخدامات هذا النوع من البطاقات عام ١٩٩٢ م عندما تم استخدامها في بطاقات الخصم Debit cards على نطاق واسع داخل فرنسا فيما كان يسمى بـ Carte Bleue، حيث كان يكفي لسداد أي مدفوعات أن يتم إيلاج البطاقة بوحدة إلكترونية عند التاجر مع إدخال الرقم السري لحاملها ليتم خصم القيمة منها مباشرة، حيث اعتبرت هذه البطاقة كحافظة، نقود إلكترونية مخزن على شريحتها قيمة ما تساويه من نقود ولا تستوجب بالضرورة وجود رصيد أو حساب لصاحبها لدى البنك.

كما شهدت حقبة التسعينيات تطوراً من نوع آخر في استخدام الشرائح الذكية في الهواتف المحمولة التي تعمل بنظام GSM على نطاق واسع في أوربا ثم باقى أنحاء العالم.

وفي عام ١٩٩٣م قامت المؤسسات المالية الدولية فيزا، ماستر يوروباي[١] بتطوير وتحديد المواصفات والمعايير الخاصة ببطاقات الدفع الذكية، بنوعيها الائتمان Credit أو الخصم Debit وكان أول إصدار من هذه المعايير ١٩٩٤م وتم تحديثها مؤخرا عام ٢٠٠٤م[٢].

---

(١) Euro pay مؤسسة مالية أوربية تضم فى عضويتها بنوكاً فى ست وعشرين دولة أوروبية تصدر بطاقة Euro card

(٢) تسمح هذه المعايير لهذا النوع من البطاقات بالتوافق مع مختلف التقنيات والنظم المطبقة فى مختلف دول العالم، وذلك طبقا لمواصفات كل من : ==

وتتميز هذه البطاقات بما يلي :

١ ـ السعة الهائلة لتخزين البيانات والمعلومات

حيث توفر تكنولوجيا الرقائق إمكانية الجمع بين أنواع مختلفة[١] التطبيقات والاستخدامات على البطاقة الواحدة، وبذلك فهي توفر المزيد من الملاءمة لحاملها، فبالإضافة لتخزين اسم صاحبها ورقم حسابه وبيانات البنك، فإن هذه التكنولوجيا تسمح بإضافة معلومات أخرى على البطاقة نفسها مثل معلومات عن هوية حامل البطاقة فضلا على التطبيقات البيومترية مثل فصيلة الدم والبصمة . . . الخ .

==أ ـ EMV (Euro pay , Master card and Visa) وهى مواصفات خاصة بالبطاقات الذكية قامت بتطويرها المؤسسات المالية الثلاثة سالفة الذكر، وقد صممت هذه المواصفات خصيصا لتحقيق خاصية التوافق للبطاقات ذات الرقائق بنوعيها الائتمان والخصم فى جميع أنحاء العالم راجعhttp//www.emvco.com

ب ـ Global Platform، وهى عبارة عن منظمة تضم فى عضويتها مؤسسات مالية دولية وشركات صناعية تزيد عددها على خمسين شركة ومؤسسة مالية ودولية متخصصة فى صناعة تكنولوجيا الرقائق وتطبيقاتها مثل الأجهزة الخاصة بقراءة وتشفير البيانات على الشرائح الذكية، وبرامج الحاسب الآلى المرتبطة بها وذلك بهدف تحقيق التناغم التكنولوجي بين جميع الأدوات والبرامج المتعلقة بالبطاقات الذكية . راجع http://www.globalplatform.org .

(١) فى هونج كونج وعلى سبيل المثال« قام احد البنوك الكبرى بالتعاون مع إحدى شركات التكنولوجيا بطرح بطاقة متعددة الاستخدامات تتيح لحاملها عدة خدمات منها إمكانية سداد قيمة مشترياته، دخول المباني المختلفة، كما يمكن استخدامها أيضا كإثبات لتحقيق الشخصية . . حتى إن بعض الخبراء الفنيين قد أطلق على هذا النوع من البطاقات « أنها الحل الذى يبحث عن مشكلة» .

٢ ـ الأمان

تحتوي البطاقة على خصائص أمان متطورة مثل خاصية تشفير البيانات التي تحول دون أي استخدام غير سليم للبطاقة، وبذلك هي أقل عرضة لعمليات التزوير والاحتيال، كما أن لكل بطاقة رقما سرياً يحميها لا يعرفه إلا حامل البطاقة فقط وفي تطبيقات بعض البنوك يمكن لحامل البطاقة تغيير الرقم السري الخاص بالبطاقة الذكية مع احتفاظه بها دون مراجعة موظفي البنك.

٣ ـ السرعة

وفقا للخصائص الأمنية السابقة فإنه يمكن إجراء المعاملات دون الحاجة لقيام التاجر بالاتصال بالبنك مما يعنى سرعة إجراء المعاملات.

ثانياً: التجارة الإلكترونية

والتجارة الإلكترونية Ecammerce تعني قيام الأطراف التجارية باستخدام وسائل الاتصال الحديثة كالحاسب الآلي وشبكات الإنترنت لتبادل المعلومات وإتمام الأعمال وإبرام الصفقات.

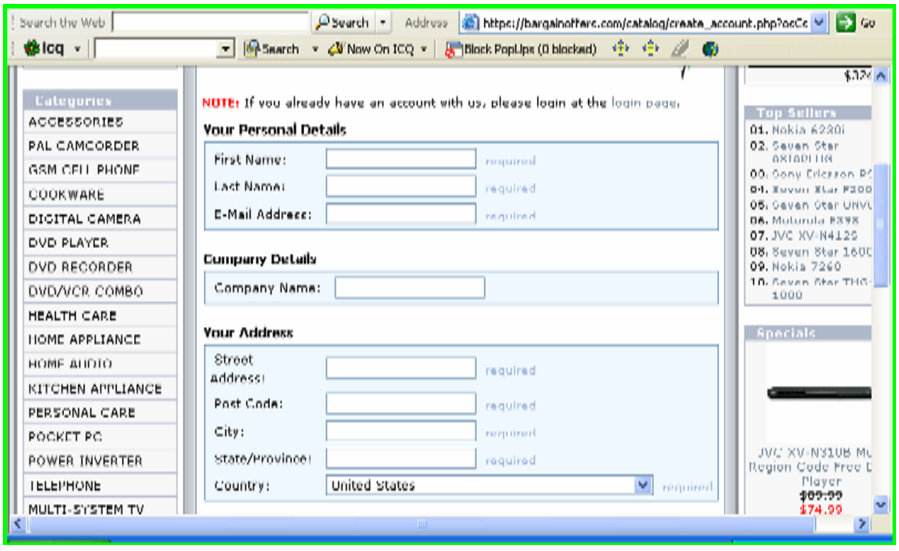
ولم تعد التجارة الإلكترونية مجرد أسلوب جديد للتجارة وتوسيع حجم الأسواق المتاحة، بل أصبحت ضرورة ملحة لجميع المؤسسات الصناعية والتجارية والخدمة التي تبحث عن زيادة قدرتها التنافسية في عصر تكنولوجيا المعلومات والذي يرفض الاعتراف إلا بالكفاءة والجودة والسعر المناسب والخدمة الجيدة.

والتجارة الإلكترونية إما أن تكون علاقة بين منتج ومستهلك وهو ما يطلق عليه Business to consumer أو B2C أو أن تكون علاقة بين شركة تجاه أخرى وهو ما يطلق عليه Business to Business أو B2B.

وما يعنينا هنا هو النموذج الأول حيث يعد هو النوع الأكثر شيوعا على المستوى الدولي، حيث يقوم مستخدم الشبكة بالتجول بين العديد من المواقع فيمكنه الشراء مباشرة أو الاشتراك في النوادي الخاصة ومشاهدة بعض الأفلام أو اللعب ببعض الألعاب نظير مبلغ من المال، أو إجراء عملية تحميل لأحد برامج الحاسب الآلي على الجهاز الذي يستخدمه Dawnlaud، والتعامل هنا يكون من خلال بطاقة الدفع الإلكترونية الخاصة بالمستخدم.

ويكفي لإجراء تلك العملية أن يتم الدخول إلى موقع المحل أو الشركة ثم اختيار السلعة المراد شراؤها، وفي هذه الحالة يظهر على الشاشة نموذج يتم ملؤه ببيانات بطاقة الدفع الإلكتروني الخاصة بالمشتري وعنوانه وتاريخ صلاحية البطاقة حيث تقوم الشركة العارضة بعد ذلك بخصم قيمة السلعة من بطاقة الدفع وإرسالها إلى عنوان المشتري الذي تمت كتابته.

صورة لصفحة أحد مواقع التسوق ببطاقات الدفع الإلكترونى على شبكة الإنترنت



ويشير أحد التقارير[1] إلى أن حجم التجارة الإلكترونية على مستوى العالم وفقا لنموذج B2C عام ٢٠٠٤م كان على النحو التالي :

١ ـ الولايات المتحدة ٣,٢ تريليون دولار أمريكي

٢ ـ آسيا والباسفيك ١,٦ تريليون دولار أمريكي

٣ ـ غرب أوروبا ١,٥ تريليون دولار أمريكي

٤ ـ أوروبا الشرقية والشرق الأوسط ٦٨,٨ مليون دولار أمريكي

٥ ـ أمريكا اللاتينية ٨٢,٠ مليون دولار أمريكي

وقد انتشرت وازدهرت عمليات التجارة الإلكترونية بشكل كبير خلال العامين الماضيين وزاد اعتماد مستخدمي الشبكة على بطاقة الدفع الخاصة بهم كوسيلة لسداد مشترواتهم عبر شبكة الإنترنت، وكان من الطبيعي أن تظهر أنماط إجرامية جديدة لم تكن معروفة من قبل استهدفت مستخدمي الشبكة وبطاقاتهم الائتمانية وذلك على النحو الذي سيتم إيضاحه في الفصل الثالث من هذه الدراسة .

ثالثاً: التحويلات المصرفية عبر شبكة الإنترنت

صاحب التطور الذي لحق بنظم التجارة الإلكترونية تطور من نوع آخر شهدته العلميات المصرفية الإلكترونية، وظهرت الخدمات المصرفية عبر شبكة الإنترنت، من خلال ما يسمى بالـ Online Banking ، حيث اتجهت العديد من البنوك على مستوي العالم إلى إنشاء مواقع لها على شبكة الإنترنت والسماح لعملائها بالولوج إلى تلك المواقع والدخول على حساباتهم المصرفية من خلال كلمة مرور خاصة Password، وإعطاء الأوامر

(١) تقرير فورستر مؤسسة دولية للبحوث الاقتصادية http://www.forrester.com

للبنك لسداد مدفوعاتهم، أو إجراء تحويلات نقدية لحسابات عملاء آخرين في ذات البنك، أو لدى بنوك أخرى، ثم ظهرت بعد ذلك العديد من المواقع التي تخصصت في تقديم خدمات مصرفية فيما يسمى ببنوك الإنترنت أو الـ Internet Banking وهى بنوك افتراضية لا وجود لها في الواقع سوى الموقع الخاص بها، وتقبل الاشتراك فيها من أي فرد أو مؤسسة وتسمح لمشتركيها بتغذية حساباتهم لديها من خلال تحويلات نقدية من بنوك أخرى أو من خلال بطاقات الدفع الإلكتروني الخاصة بالمشتركين.

١ ـ بطاقة E-Gold

انتشر خلال السنوات الأخيرة نوع من بطاقات الخصم Debit Cards مدفوعة القيمة Prepayed ذات فئات مختلفة، ومع انتشار هذا النوع من البطاقات لجأت العديد من المواقع المتخصصة في إجراء التحويلات الإلكترونية عبر شبكة الإنترنت إلى تسويق تلك البطاقات، واشهر هذه البطاقات هي بطاقة E-Gold، وهى بطاقة ممغنطة تصدر من العديد من المواقع برعاية مؤسسة ماستركارد الدولية، ويمكن الحصول عليها من خلال الاشتراك في أحد هذه المواقع[1]، وسداد قيمتها عن طريق التحويلات النقدية أما إليكترونيا E-transaction أو من خلال تحويلات بنكية عادية Wire transfer، لتصل إلى المشترك بعد ذلك بالبريد العادي على عنوان منزله في أي دولة في العالم، برغم أن رصيد هذه البطاقة محدد بقيمتها التي لا تزيد عن مائة دولار أمريكي، إلا أنه يمكن زيادة هذا الرصيد بأية مبالغ أخرى يتم إضافتها لحساب المشترك لدى الموقع الذي قام بشراء البطاقة منه. وبالطبع ونظرا لأن هذه البطاقة تصدر برعاية مؤسسة ماستركارد الدولية وهى مؤسسة

(١) أشهر هذه المواقع هو موقع http://www.inerimentalgold.com

مالية تمارس نشاطها حول العالم، فإن صلاحية استخدام هذه البطاقة «خاصة في عمليات السحب النقدي» من خلال آلات الصرف النقدي ATMs أصبح متاحًا حول العالم أيضا.

ونظراً لعدم محدودية نطاق استخدام هذه البطاقات حول العالم، فقد وصف هذا النظام بأنه وسيلة مثلى للاحتيال وإخفاء الأموال بل وغسلها أيضا وهو ما سوف نوضحه فيما بعد عند إلقاء الضوء على بعض نماذج من القضايا التي تم ضبطها في مصر في هذا المجال إلا أن المسئولين عن هذا النظام يتعاونون بشكل جيد مع أجهزة المكافحة في العديد من دول العالم.

٢ ـ خدمة Pay pal

وأشهر هذه المواقع هو موقع http://www.paypal.com وهو موقع أمريكي بدأ نشاطه عبر الشبكة عام ١٩٩٩م ويسمح للأفراد المشتركين بتحويل الأموال من والى بعض عن طريق البريد الإلكتروني، وقد بدأت هذه الخدمة داخل الولايات المتحدة فقط، أما اليوم فقد وصل عدد الدول التي يمكن أن يستفيد رعاياها من هذه الخدمة إلى أكثر من مائة دولة حول العالم بعملات، دولار أمريكي، كندي، استرالى، ين ياباني، يورو، استرليني ويقوم هذا الموقع بدور اللاعب الرئيس في العديد من تطبيقات التجارة الإلكترونية، حيث يتيح لمشاركيه إجراء عمليات التسويق عبر الشبكة دون الحاجة

لاستخدام بيانات بطاقات الدفع الإلكتروني الخاصة بهم، كما انه يمكن من خلال هذا الموقع أيضا إجراء تحويلات نقدية من بطاقات الدفع الإلكتروني من وإلى أي فرد داخل الدول التي تستفيد بخدمات هذا الموقع(*).

من التطورات التكنولوجية الهامة أيضا ما قامت به شركتا ويسترن يونيون western union، مانى جرام Money Gram وهما شركتان أمريكيتان متخصصتان في تحويل الأموال بإتاحة خدمة تحويل الأموال إلكترونياً من خلال موقعيهما على شبكة الإنترنت(1).

وتتميز الخدمات المصرفية التي تقدم من خلال مواقع الإنترنت بالسرعة والأجور المنخفضة، بعضها مجانا، كما أنها تقدم خلال الـ الأربع والعشرين ساعة طوال أيام الأسبوع وأيضا في أيام العطلات والإجازات الرسمية.

(*) ولضمان عدم إساءة استخدام هذه الخدمة فى علميات غسل الأموال المتحصلة من أنشطة غير مشروعة، فقد تم تقسيم البنوك المشاركة فى هذه الخدمة بحسب الدول التى تطبق المعايير الدولية Fatf Recommendations فى هذا المجال الى ثلاث مجموعات المجموعة الأولى : يسمح لهم بإجراء التحويلات واستلام الأموال من وإلى البنوك المحلية والأمريكية دون قيود . المجموعة الثانية : يسمح لهم بإجراء تحويلات من خلال شيكات ورقية او حسابات مصرفية لدي بنوك أمريكية ولا يسمح لهم بالتحويلات الاليكترونية الى بنوكهم المحلية . المجموعة الثالثة : لا يمكنهم إجراء التحويلات الاليكترونية أو استلام شيكات ورقية مسحوبة عليها، بينما يمكنهم إجراء تلك التحويلات الى بنوك أمريكية راجع http://www.paypal.com

(1)http:// www.westernunion.com
http:// www.moneypram.com

٢ . ٣ صور العلاقة بين العميل والبنك

تتعدد صور العلاقة بين البنك والتاجر ، فهناك العديد من التجار الذين يستوجب عليهم إجراء العملية أو الحركة باستخدام البطاقات بشكل مباشر ، بينما هناك العديد من التجار الذين يسمح لهم بقبول السداد بالبطاقات عن طريق الـ Mailorder أو عن طرق الهاتف شريطة أن ينص العقد المبرم بين البنك والتاجر على ذلك .

كما أن هناك سقفا ائتمانيا« Floor limit» لكل عملية يتم تحديده للتاجر في العقد المبرم بينه وبين البنك ، ويختلف السقف الائتماني هنا بين تاجر وآخر .

ولكن ما هي حدود مسئولية البنك ؟ وماذا يجب عليه؟ وأيضا ما هي مسئولية التاجر في هذا النشاط ذلك ما سوف نوضحه :

٢ . ٣ . ١ حدود مسئولية والتزامات البنك مع التاجر

١ ـ يجب على البنك التأكد من حسن سمعة التاجر وقدرته على الوفاء بالتزاماته المالية .

٢ ـ عمل زيارة ميدانية لمحل التاجر ـ للوقوف على نشاطه والتحقق من سلامة ومطابقة الرخص والمستندات مع نوع النشاط المصرح له .

٣ ـ توقيع عقد مع كل تاجر على حده .

٤ ـ قبول الحركات التجارية الواردة من خلال هؤلاء التجار ، بحسب نشاط كل منهم .

٥ ـ متابعة الحركات التي يتم إجراؤها من خلال التجار ، وأنها في حدود السقف الائتماني Floor limit المحدد لكل تاجر .

٦ ـ سداد مجموع الحركات المقدمة من التاجر بعينة « في فترة زمنية لا تتعدي يوم العمل التالي من تقديم الإشعارات الدالة على إتمام هذه الحركات لدى التجار .

٧ ـ وقد يؤجل السداد لفترة زمنية قصيرة للتحقق من مصداقية الحركات المقدمة ، ويتم السداد نقدا أو بشيكات أو بالإضافة لحساب بنكي .

٨ ـ تزويد التجار بإشعارات الخصم ومواد الدعاية والماكينات اليدوية والإلكترونية التي تحمل العلامات التجارية للبنك والمنظمات والمؤسسات المالية الدولية Visa , Master Card - Amerecan Express

٩ ـ حفظ ملفات التجار كاملة ومتضمنة جميع البيانات التي يمكن الرجوع إليها في حالة إجراء تحريات ، وذلك لمدة لا تقل عن سنتين من تاريخ إنهاء التعاقد مع التاجر .

١٠ ـ مراقبة ومتابعة الحركات الناتجة عن نشاط التجار للحد من عمليات التزوير والاحتيال .

٢ . ٣ . ٢ مسئوليات والتزامات التاجر

١ ـ يلتزم التاجر بقبول جميع بطاقات الدفع الإلكتروني التي يتضمنها عقده مع البنك Visa, Master Card . . . . الخ دون تمييز

٢ ـ يلتزم البنك بعرض العلامات التجارية للمنظمات الدولية ، كإعلان للجمهور بأنه يقبل التعامل بهذه البطاقات كوسيلة للسداد .

٣ ـ يجب على التاجر أن يتأكد من تاريخ بدء الصلاحية وتاريخ الانتهاء على كل بطاقة تقدم إليه ، وفي حالة الخصم على البطاقات باستخدام الماكينات الإلكترونية POS عن طريق قراءة الشريط الممغنط للبطاقة على التاجر أو البائع أن يقارن رقم البطاقة البارز

على وجه البطاقة وبين رقم البطاقة الظاهر على إشعار الخصم الصادر عن الماكينة الإلكترونية.

٤ـ يلتزم التاجر بعدم خصم قيمة حركات غير صحيحة أو لم يتم الموافقة عليها من قبل حاملي البطاقات، ويعد التاجر مسئولا عن أفعال موظفيه العاملين لديه طوال فترة عملهم.

٥ ـ كما يلتزم التاجر بأن يقدم إشعارات الخصم من بطاقات الدفع الإلكتروني التي تمت نتيجة نشاطه التجاري فقط، ولا يحق له المطالبة بقيمة إشعارات خصم لعمليات تمت من خلال تاجر آخر.

٦ ـ لا يحق للتاجر أو البائع مطالبة المشتري وحامل البطاقة بمصاريف إضافية تزيد على سعر السلعة أو الخدمة المعلن عنها.

٢ .٣ .٣ الأجهزة والأدوات المستخدمة لدى نقاط البيع

عندما يقبل التاجر التعامل بالبطاقات، بعد أن يتعاقد مع أحد البنوك المصرح لها بذلك، يصبح عضوا في شبكة مركبة من منظمات الدفع وتكنولوجيا المعلومات التي تعمل بصورة منتظمة للتأكد من أن عملية الدفع تمت بسرعة وأمان، وبذلك يضمن التاجر الحصول على مستحقاته بصورة سريعة عن كل معاملة معتمدة يتم إجراؤها في متجره، فضلا عن حمايته ضد أي سوء استخدام للبطاقة.

وبرغم تعدد وتنوع البنوك والمنظمات الدولية المسئولة عن هذا النشاط محليا ودوليا، إلا أن الأجهزة والأدوات المستخدمة لدى نقاط البيع في المتاجر والمطاعم والفنادق.. الخ. ذات مواصفات واحدة، فعملية الدفع إما أن تتم بصورة يدوية حيث لا تكون هناك قناة اتصال بين المتجر والبنك، أو بصورة إلكترونية من خلال جهاز كهربائي متصل تليفونيا مع بنك التاجر،

وتختلف الإيصالات الدالة على إتمام عملية الشراء والدفع في الحالتين وذلك على النحو التالي :

١ ـ إتمام عملية الدفع بالطريقة اليدوية Manual transaction

وكانت هي الطريقة الوحيدة المتبعة لإتمام عمليات الدفع بالبطاقات حتى بداية الثمانينيات وقبل انتشار وتطور نظم الاتصالات وشبكات المعلومات » وتتمثل تلك الطريقة في أن يقوم البنك بتسليم التاجر المتعاقد معه ختامة يدوية Manual imprinter مصنوعة من المعدن والمطاط مطبوع عليها اسم التاجر ورقمه لدى البنك بالأحرف والأرقام البارزة، وكذا كمية من الإيصالات تحمل اسم البنك وشعار المنظمة الدولية المعدة خصيصا للتعامل مع تلك الختامة، وكل إيصال عبارة عن أصل ملصق به صورتان مصنوع من ورق ذى خاصية كاربونية تسمح بنقل أية بيانات تدون على الأصل إلى كل من الصورتين .

أما الختامة اليدوية Manual imprinter فهي كما سبق أن أشرنا عبارة عن قالب من المعدن مركب عليه مقبض يدوي منزلق ومزود باسطوانة مطاطية كما هو موضح بالشكل التالي :

ولدى قيام حامل البطاقة بتحديد مشترياته يتقدم للتاجر ببطاقته ليقوم بدوره بعد التحقق من شخصية حاملها بإتباع الخطوات التالية :

١ ـ كتابة القيمة الإجمالية للمشتريات بخط يده في الموضوع المحدد بأحد الإيصالات المسلمة له من البنك .

٢ ـ تثبيت البطاقة في الموضع المحدد لها على الختامة والذي يكون الجهة المقابلة للموضع المطبوع عليه بيانات التاجر ورقمه لدى البنك بالأحرف البارزة .

٣ ـ وضع الإيصال في المكان المحدد بالختامة .

٤ ـ سحب المقبض «يدويا» يمينا لطباعة بصمة البيانات البارزة للبطاقة على الإيصال ، وإعادته يساراً لطباعة بصمة بيانات التاجر على ذات الإيصال وذلك بتأثير الضغط التلقائى للأسطوانة المطاطية .

٥ ـ يطلب من حامل البطاقة التوقيع على الإيصال ومطابقته على توقيعه السابق على ظهر البطاقة للتحقق من شخصيته .

٦ ـ إعادة البطاقة للمشتري وتسليمه صورة من الإيصال الدال على العملية وقيمتها .

٧ ـ تسليم أصل الإيصال للبنك للحصول على مستحقاته مع الاحتفاظ بصورة من الإيصال للرجوع إليها عند الحاجة .

ورغم انتشار الأجهزة الإلكترونية لدى العديد من نقاط البيع في مختلف دول العالم، إلا أن الأجهزة اليدوية مازالت مستخدمة في العديد من تلك الدول وإن كانت على نطاق محدود، إلا أنها لا زالت مطبقة خاصة في المناطق التي لا تتوافر فيها خطوط اتصالات كما أنها موجودة لدى العديد من التجار الذين يتوافر لديهم أجهزة إلكترونية توخياً لتعطل الجهاز أو خطوط الهاتف(*).

٢ ـ إتمام عملية الدفع بالطريقة الإلكترونية POS transaction

وهنا يقوم البنك بتسليم التاجر المتعاقد معه وحده إلكترونية تعمل بالكهرباء مزودة بمودم Modem يسمح للوحدة بالاتصال بالحاسب الآلي الخاص بالبنك من خلال خطوط الهاتف ولها شاشة ضوئية يمكن أن يظهر عليها عبارات ورسائل مختصرة حتى ثمانية وأربعين، وفالقاً طوليا مزوداً برأس قارئ بيانات الشريط الممغنط وبها مفاتيح تشغيل وحاسبه آلية وبها طابعة نقطية تعمل على شريط بنظام Dot-matrix Roll printer البعض ذو طبقتين والبعض الآخر من طبقة واحدة لطباعة الإيصال الدال على إتمام العلمية آليا من أصل وصورة.

ولدى قيام حامل البطاقة هنا بتحديد مشترواته يتقدم للتاجر ببطاقتة ليقوم بدوره بعد التحقق من شخصية حاملها بإتباع الخطوات التالية:

١ ـ التحقق من أن الوحدة الإلكترونية POS متصلة بالكهرباء وخط الهاتف.

٢ ـ تحقيق الاتصال مع البنك من خلال لوحة المفاتيح.

(*) دأب العديد من مسئولي الفنادق وشركات السياحة ومعارض تأجير السيارات على استخدامها في الحصول على بصمة البطاقة الخاصة بعملائها على إيصال خال من أية بيانات عند بدء التعامل لضمان الحصول على مستحقاتهم كاملة بعد إتمام تقديم الخدمة.

٣ ـ إدخال قيمة مشتريات حامل البطاقة .

٤ ـ تمرير البطاقة من خلال الفالق الطولى لتنتقل بياناتها الملقنة للشريط الممغنط إلى الحاسب الآلي بالبنك : «الذي يعمل بصفة مستمرة طوال الأربع والعشرين ساعة ضمن المعلومات الخاصة بالمنظمة الدولية» حيث تنتقل بيانات البطاقة والعملية خلال تلك الشبكة وفق مسارات محددة إلى أن تصل إلى البنك المصدر للبطاقة ليتم التحقق من سلامة العملية وإتمامها أو الاعتراض عليها

وهنا تظهر على شاشة الوحدة الإلكترونية إحدى الرسائل الآتية :

أ ـ الموافقة Approval

ب ـ الرفض Decline

جـ ـ مراجعة البنك مصدر البطاقة Refer

د ـ أمر بسحب البطاقة Pick up إذا كانت البطاقة مبلغاً بسرقتها أو فقدها .

صور لوحدات POS المستخدمة لدى التجار



٥ ـ وفي حالة الموافقة على إتمام العملية فإن الوحدة تقوم تلقائياً بطباعة إيصال صغير من أصل وصورة ليقوم حامل البطاقة بالتوقيع عليهم ، ويتولى البائع مطابقة التوقيع هنا على التوقيع الوارد على ظهر البطاقة ليتحقق من شخصية حامل البطاقة ويقوم بتسليمه مشترياته مع صورة من الإيصال .

صورة ايصال مخرج من وحدة (POS)

٦ ـ يقوم البائع بمراجعة البنك للحصول على مستحقاته عقب ذلك مع احتفاظه بالإيصال أو تسليمه للبنك حسب النظام المتفق عليه .

أجهزة وأدوات قراءة البطاقات الذكية

بدأت منذ عدة سنوات العديد من الشركات المتخصصة في صناعة هذا النوع من التكنولوجيا في إنتاج العديد من الأجهزة والأدوات التي تسمح بقراءة الشرائح الذكية والتعامل معها ، وذلك طبقا لمعايير كل من Globalplatform - EMV منها أجهزة نقاط البيع POS ، ماكينات الصرافة الآلية ATMs وكذا بعض الأدوات الأخرى التي يمكن استخدامها كملحقات لأجهزة الحاسبات الآلية الشخصية والمحمولة ، كما ظهرت بعض أجهزة الحاسب الآلي مزودة بوحدة لقراءة هذا النوع من البطاقات ، وقامت شركات أخرى بإنتاج لوحات المفاتيح مزودة بهذه الخاصية keyboard smart card Reader ، ونظرا لأن الانتقال إلى مرحلة انتشار البطاقات الذكية ، هي عملية

تدريجية(*)، لذا قامت البنوك في مختلف دول العالم بطرح بطاقاتها المغنطة مزودة بالشرائح الذكية، ومن المتوقع أن تستغرق عملية الانتقال عدة سنوات، والى أن يتم ذلك سوف تظل البطاقات المغنطة مقبولة لدى كافة نقاط البيع في كل أنحاء العالم.

صورة لوحدات POS تستخدم مع البطاقات الذكية لدى التجار



٣ ـ جهاز إدخال الرقم السري Pin pad

بعد أن زادت صور التلاعب المصاحبة لنظم الدفع الإلكترونية في منتصف التسعينيات قامت بعض شركات الإلكترونيات بإنتاج وحدة

(*) تختلف سرعة وإجراءات التحول من البطاقات المغنطة الى البطاقات الذكية من بنك لآخر ومن دولة لأخرى وذلك بحسب مدى انتشار جرائم الاحتيال والتزوير فى الدولة وما تتعرض له البنوك من خسائر، وذلك بالقياس للتكلفة العالية التي قد تتكبدها البنوك والمؤسسات المالية في عملية التحول بين النظامين، الا أنه من المؤكد أن تحول البنوك والمؤسسات المالية فى دولة ما إلى البطاقات الذكية سوف يؤدي حتمًا إلى هجرة جرائم الاحتيال والتزوير في بطاقات الدفع الاليكترونية إلى الدول الأخرى التى مازالت تطبق نظم التعامل بالبطاقات المغنطة، وخير دليل على ذلك ما حدث فى ماليزيا بعد ان قامت البنوك والمؤسسات المالية بها بالتحويل الى تطبيقات تكنولوجيا البطاقات الذكية حيث انخفضت جرائم التزوير والاحتيال المرتبطة ببطاقات الدفع الاليكتروني بشكل كبير، بينما زادت بنفس النسبة تقريباً في دولة تايلاند الملاصقة لها حدوديًا، نظرا لضعف انتشار هذه التكنولوجيا في الدولة الأخيرة.

إلكترونية صغيرة الحجم يمكنها الاتصال «سلكيا أو لاسلكيا» بوحدات نقاط البيع الإلكترونية POS وذلك بهدف تمكين حامل البطاقة من إدخال الرقم التعريفي «السري» بصورة آمنة، وهى وحدة لا تحتاج إلى مصدر كهربائي، حيث يقوم البائع بإتاحة الفرصة للمشتري لإدخال الرقم التعريفي الخاص به المكون من أربعة أرقام Pin [1] الذي لا يعرفه سواه والعملية هنا لا تتم إلا إذا كان هذا الرقم صحيحا.

صورة لوحدات إدخال الرقم السري المستخدمة لدى التجار

ويجب أن نوضح هنا أن هذه الخدمة Pin pad يتم إتاحتها بمعرفة البنك بناء على طلب التاجر ومن ثم فإن كافة العمليات التي يجب أن تجرى في هذا المحل يجب أن تكون مقترنة باستخدام الرقم التعريفي الصحيح لها وبدونه لا تتم العملية مطلقا.

٤ ـ أجهزة الصراف الآلي Automated Teller Machines ATMs

سبق أن أوضحنا أن بطاقات الدفع الإلكتروني قد انتشرت وتنوعت استخداماتها كبديل للنقود عند نقاط البيع، إلا أن أعوام ١٩٦٧م، ١٩٧٢م، ١٩٧٣م كانت قد شكلت نقاطاً مهمة في التطور التاريخي لاستخدام هذا النوع من البطاقات حين طورت مؤسسة دي لارو

(١) اختصار لـ Personal Identification Number

Dela Rue أول ماكينة آلية لصرف النقود لحساب بنك باركليز بلندن وتم تطوير الجيل الثاني منها عام ١٩٧٢م لتعمل من خلال شبكات الاتصال باستخدام البطاقات ذات الشريط الممغنط وسرعان ما انتشرت عام ١٩٧٣م بعد أن قامت مؤسسة اميركارد Americard Bank بتأسيس أول نظام إليكتروني لتشغيل البطاقات، واليوم تشكل شبكات آلات الصراف الآلي أحد أهم القنوات المصرفية التي تضمها البنوك والمؤسسات المالية في مختلف دول العالم، حيث تم التوسع في استخدامها لإجراء كافة المعاملات المصرفية كالسحب والإيداع ومعرفة الرصيد وطلب كشف الحساب في أي وقت على مدار الأربع والعشرين ساعة طوال أيام الأسبوع.

وحدات من الصراف الآلي ATMs

ويعتمد تأمين نظام عمل تلك الآلة على كل من البطاقة « وتعد بمثابة مفتاح للدخول» والرقم التعريفي الشخصى PIN المكون من أربعة أرقام.

الفصل الثالث

أخطار بطاقات الدفع الإلكتروني

٣. أخطار بطاقات الدفع الإلكتروني

رأينا كيف انتشرت بطاقات الدفع الإلكتروني في كافة أنحاء العالم وتوغلت في كافة الأنظمة النقدية، نظراً للتيسيرات التي تمنحها لحاملها ليتمكن من شراء أي سلعة أو منتج من أي نقطة بيع في العالم وبأي عملة. وكيف أثرت تكنولوجيا المعلومات ونظم الاتصالات في التطور الذي لحق بتطبيقات استخدامات تلك البطاقات حول العالم.

وكان من الطبيعي أن تظهر أشكال إجرامية جديدة اتخذت من بيئة نظم الدفع الإلكتروني وسطاً لتنمو فيه وتزدهر، الأمر الذى شكل خطراً داهماً على هذه الصناعة وهدّد خطط المؤسسات المالية الدولية في النمو بهذه النظم، وتعددت تلك الأشكال الإجرامية وتنوعت مخاطرها، وزاد من خطورتها قيام بعض جماعات الجريمة المنظمة من محترفي ارتكاب هذا النوع من الجرائم من استغلال تفاوت الحماية التشريعية بين دول العالم المختلفة، بحيث أصبحت تميل إلى التركيز في ارتكاب هذه الجرائم في الدول الأقل حماية. وساعدت بيئة تكنولوجيا المعلومات هؤلاء الأفراد والجماعات على ابتكار كافة وسائل الاحتيال والخداع والتخفي أثناء ممارسة وارتكاب تلك الأنشطة.

والحقيقة المؤكدة أن ما قد يتوافر من إحصاءات عن تلك الجرائم لا تعكس بالضرورة حجم هذا النشاط في الواقع، نظراً لأن العديد من الضحايا لا يقومون بمراجعة كشوف الحساب الخاصة ببطاقاتهم، كما أن غالبية البنوك والمؤسسات المالية قد دأبت على الإحجام عن الإبلاغ عن تلك الوقائع والاكتفاء بعلاج الأمر داخلياً أو التسوية مع العميل حفاظاً على السمعة وعدم تعريض موظفيهم للمساءلة القانونية.

والواقعة التي تم ضبطها بمعرفة الشرطة الأسترالية عام ٢٠٠٠م هي خير دليل على ذلك حيث كان قد ورد إلى الإدارة العامة لمباحث الأموال العامة عن طريق إنتربول القاهرة برقية إنتربول كانبرا بأستراليا تتضمن اكتشاف ارتكاب وقائع لعمليات نصب واحتيال باستخدام بطاقات ائتمان مزورة في أستراليا، وذلك عن طريق استخدام بعض برامج الحاسب الآلي ومواقع على شبكة الإنترنت، حيث أمكن الحصول على بيانات عن بطاقات صالحة للاستخدام خاصة بالعديد من البنوك في دول مختلفة، ثم تلقين هذه البيانات إلى بطاقات ائتمان مزورة وتوزيعها على المهربين الذين قاموا باستخدامها في شراء بضائع والتصرف فيها وتحويل عائداتها إلى حسابات مصرفية في ماليزيا.

وقد بلغت جملة المبالغ التي تم الاستيلاء عليها بهذا الأسلوب ما يزيد على الخمسين مليون دولار أمريكي، وقد تمكنت الشرطة الأسترالية من تحديد تشكيل عصابي في ماليزيا وراء تلك الوقائع التي تركزت في أستراليا، كما ثبت أن ارتكاب تلك الوقائع قد تم باستخدام أرقام بطاقات ماستركارد صحيحة منسوبة لبعض البنوك في دول السويد، النرويج، ألمانيا، إنجلترا، سويسرا، مصر حيث اتضح أن جملة ما تم إجراؤه من عمليات احتيالية باستخدام أرقام بطاقات ائتمانية صادرة من أحد البنوك المصرية «وهو البنك المصري الوحيد في تلك الواقعة »قد بلغت ١,٩٠٠,٠٠٠ مليون وتسعمائة ألف دولار أمريكي، استخدم فيها أرقام ما يزيد على أربعمائة بطاقة تخص عملاء البنك[١].

---

(١) من أرشيف الإدارة العامة لمباحث الأموال العامة.

وألقت الشرطة الأسترالية القبض على عدد أربعة عشر فرداً من المتورطين في تلك الوقائع وهم من جنسيات ماليزيا، سنغافورا، أستراليا وبعضهم ذو جنسيات مزدوجة وأسماء منتحلة. وقد تحمل البنك تلك الخسائر ولم يقم بالإبلاغ عنها.

والأشكال الإجرامية المصاحبة لنشاط بطاقات الدفع الإلكتروني منها ما يتم ارتكابه بشكل مباشر ويكون محله إما البطاقة أو مستندات استخراجها أو التاجر أو البنك، ومنها ما يتم ارتكابه بشكل غير مباشر مستهدفاً بيانات البطاقات لدى حاملها أو البنك المصدر لها، ونظراً لأن تلك الجرائم قد اتخذت صوراً نمطية في كافة الدول لذا فإننا سنتناولها بشيء من التفصيل في ثلاثة أقسام، فنتحدث في القسم الأول عن الأنماط الإجرامية المختلفة لجرائم بطاقات الدفع الإلكتروني ثم نتحدث عن أثر التطور التكنولوجى على جرائم بطاقات الدفع الاليكترونى في قسم ثان، بينما قمنا بتخصيص الثالث للتحدث عن الخسائر المادية والمردودات السلبية لهذا النشاط.

٣ .١ الأنماط المختلفة لجرائم بطاقات الدفع الإلكتروني

تعددت الأنماط الإجرامية التي صاحبت نشاط بطاقات الدفع الإلكتروني خلال السنوات الماضية، وبالرغم من أن بعض تلك الحالات كانت فردية، إلا أن حالات أخرى قد تكررت وانتشرت وأخذت شكل الظاهرة وتخطت آثارها حدود الدول، وهي كما يلي:

- استخدام البطاقة المسروقة أو المفقودة.
- استصدار بطاقات صحيحة بمستندات مزورة.
- تزوير إشعارات المبيعات المستخدمة مع هذا النظام.

ـ تواطؤ التاجر أو البائع، والتلاعب في ماكينات البيع الإلكترونية.

ـ تزوير بطاقات الدفع الإلكتروني.

ونتناول كل شكل من تلك الأشكال الإجرامية بشيء من التفصيل على النحو التالي:

٣ .١ .١ استخدام البطاقات المسروقة أو المفقودة

ويكثر هذا النوع من الجرائم في المناطق ذات الطبيعة السياحية، حيث تخصص العديد من الأفراد في سرقة بطاقات الدفع الإلكتروني من أصحابها «خاصة الأجانب» ثم استخدامها في الحصول على السلع والخدمات من المحلات والفنادق.

وعادة ما يكون استخدام هذه البطاقات في عمليات عديدة وسريعة في نفس يوم سرقتها وقبل أن يكتشف أمرها.

وبالطبع فإن هذا الأسلوب الإجرامي غالباً ما يقترن بجريمة تزوير توقيع صاحب البطاقة الأصلي على إشعارات المبيعات وتتحدد مسئولية كل من البنك المصدر للبطاقة وصاحب البطاقة الأصلي عن الاستخدام غير المشروع لها وفقاً للتوقيت الزمني الذي يتم فيه إبلاغ البنك المصدر بواقعة سرقة البطاقة أو فقدها، حيث يتحتم على البنك إيقاف العمل بالبطاقة فور ورود البلاغ إليه تليفونياً، بل إنه يقوم بإلغائها بناء على طلب العميل في غالب الأحيان.

وتكمن خطورة هذا النوع في أن غالبية الضحايا قد لا يكتشفون واقعة فقد البطاقة أو سرقتها إلا بعد مرور فترة من الزمن قد تكون كافية لاستنفاذ الرصيد أو جزء منه.

ويلجأ بعض البنوك إلى تزويد نظام الحاسب الآلي الخاص بالبنك بخاصية تسمح بإيقاف التعامل على البطاقات التي يمر عليها فترة تتراوح بين شهرين إلى ثلاثة أشهر دون استخدام، وذلك حفاظاً على أموال وأرصدة عملاء البنك بافتراض أن تكون البطاقة قد تعرضت للسرقة دون علم صاحبها.

٣ .١ .٢ استصدار بطاقات صحيحة بمستندات مزورة

وكانت هذه الحالات هي الأكثر انتشاراً خلال عقد التسعينيات حيث دأب بعض المحتالين إلى التقدم إلى أفرع بعض البنوك بمستندات إثبات شخصية مزورة للحصول على بطاقات ائتمان بأسماء منتحلة وعناوين وهمية، ويتم استخدام تلك البطاقات بمبالغ مالية كبيرة في عمليات سريعة ومتتالية.

وبالطبع فإن هذا النوع من الجرائم لا يقع إلا على بطاقات الائتمان، فلا يتصور أن يكون محله بطاقات الخصم.

وعادة ما لا يكتشف البنك تلك الواقعة إلا بعد مضي شهرين تقريباً وذلك عندما يقوم بمطالبة العميل «المحتال» بسداد قيمة كشف حساب البطاقة خلال الشهر التالي لصدورها، ولدى عدم قيام العميل بالسداد يقوم البنك بإيقاف البطاقة ومعاودة مطالبة العميل الذي لن يقم بالسداد بالطبع، وهنا يكون العميل «المحتال» قد استولى على الرصيد الائتماني للبطاقة مرتين.

وهذا النوع من الجرائم عادة ما ينطوي على جرائم تزوير محررات رسمية واستعمالها، حيث يتقدم المحتال للبنك بمستندات إثبات شخصية مزورة مثل جواز السفر أو البطاقة الشخصية وبعض المحررات الأخرى المزورة كشهادة التسجيل التجاري أو الشهادات البنكية المنسوبة لبنوك أخرى

تفيد «خلافاً للحقيقة» أن للعميل «المحتال» ودائع أو أرصدة بمبالغ كبيرة بهدف زيادة الحد الائتماني للبطاقة المزمع إصدارها.

وعادة ما يلجأ محترفو هذا النوع من الجرائم إلى استهداف أكثر من بنك لاستصدار عدة بطاقات بذات الأسلوب وبأسماء وبيانات منتحلة لتحقيق أكبر عائد ممكن خلال فترة زمنية قصيرة وقبل اكتشاف تلك الوقائع مستغلين ضعف وخبرة بعض موظفي البنوك في كشف تزوير المستندات والوثائق.

٣. ١. ٣ تزوير إشعارات المبيعات والفواتير المستخدمة مع هذا النظام

وتنطوي هذه الجريمة على خيانة أمانة من بعض العاملين أو البائعين في المنشآت والأوساط السياحية، الذين يقومون بمغافلة صاحب البطاقة «عادة ما يكون أجنبياً» والحصول على بصمتها على إشعار خال البيانات باستخدام ختامة فواتير الشراء اليدوية وإعادة ملئه بعد انصراف حامل البطاقة مع تزوير توقيع الأخير على الإشعار أو الفاتورة بما يفيد «خلافاً للحقيقة» شراءه للسلعة أو حصوله على خدمة ما بمبلغ معين، وتقديم تلك الإشعارات المزورة للبنك لصرف قيمتها.

وهذا النوع من الجرائم لا يقع أيضاً إلا مع بطاقات الائتمان «التي تحمل أرقاماً وبيانات بارزة» ولا يتصور وقوعه على بطاقات الخصم التي تخلو من البيانات البارزة ولا تصلح للتعامل مع ختامات الفواتير اليدوية.

كما أن هذا النوع من الجرائم لا يتم اكتشافه إلا عند مراجعة الضحية لكشف الحساب الوارد من البنك، والذي لا يتم في الغالب إلا بعد مضي فترة زمنية تتراوح بين شهر إلى شهرين على ارتكاب الواقعة، حيث يكتشف

صاحب البطاقة أن كشف الحساب يتضمن خصم مبالغ عن عمليات لم يقم بإجرائها، وهنا لا يكون أمامه إلا تقديم اعتراض على هذه العمليات إلى البنك المصدر للبطاقة، الذي يقوم بدوره بإرسال هذه الاعتراضات إلى بنك التاجر الذي قام بإتمام العملية «عادة ما يكون في دولة أخرى» ومطالبته بصورة من فاتورة الشراء «المزورة»، لاطلاع صاحب البطاقة الأصلي عليها الذي غالباً ما يصر على أنه لم يوقع على هذه الفاتورة، ويتضح بالفعل أن توقيعه عليها مخالف لتوقيعه لدى البنك، وهنا يتم رد المبلغ إلى صاحب البطاقة، مع خصمه من حساب التاجر لدى البنك الخاص به.

وكل الحالات التي سبق فحصها لهذا النوع من الجرائم تشير إلى أن الواقعة عادة ما ترتكب على مرحلتين:

الأولى: وفيها يتم مغافلة صاحب البطاقة والحصول على بصمتها على إشعار خال من البيانات، وتجرى هذه المرحلة بمعرفة أحد موظفي الفنادق أو المَطاعم أو المنشآت السياحية، باستخدام ختامة الفواتير اليدوية الخاصة بهذه المنشأة.

الثانية: وتتم بعد انصراف العميل «صاحب البطاقة» وغالباً ما يكون أجنبياً» وبعد مغادرته البلاد حيث يتم ملء الإشعار أو الفاتورة التي تحمل بصمة البطاقة بقيمة مالية، وتزوير توقيع صاحبها بما يفيد حصوله على خدمة أو سلعة ما، ثم استكمال العملية لدى تاجر آخر «عادة ما يكون متواطئاً مع القائم بالمرحلة الأولى» باستخدام ختامة الفواتير اليدوية الخاصة بالتاجر الأخير، الذي يتولى تقديم هذا الإشعار أو الفاتورة المزورة إلى البنك لصرف قيمتها، واقتسامها مع شريكه.

والتاجر الذي يتورط في مثل هذه الواقعة عادة ما يكون ذا نشاط إجرامي مستمر في هذا المجال حيث يتضح ذلك من خلال تعدد الاعتراضات التي وردت من بنوك أجنبية إلى البنك المتعاقد معه ذلك التاجر عن عمليات احتيالية تم إجراؤها باستخدام ختامة الفواتير الخاصة به «في المرحلة الثانية» والتي تحمل بصمة بيانات محله ورقمه لدى البنك.

٣ .١ .٤ تواطؤ التاجر أو البائع والتلاعب في ماكينات البيع الإلكترونية

وعملية تواطؤ التاجر أو البائع هنا قد تكون بالاشتراك مع صاحب البطاقة وقد تكون في غفلة عنه«كما في حالة تزوير الإشعارات والفواتير» وتكثر الحالة الأولى بين حاملي البطاقات من الأجانب والسائحين الذين يقومون باستخدام بطاقاتهم إلى أن يتم استنفاذ رصيدها الائتماني الشهري، فيلجأ حامل البطاقة إلى أحد التجار المشبوهين لإجراء بعض عمليات الشراء الوهمية ويحصل لنفسه على نسبة نقدية من قيمة الفاتورة بينما يحصل التاجر على الباقي نظير إتمام تلك العمليات، وتحصيل قيمة الفواتير كاملة بعد ذلك من البنك.

وعادة ما تكون تلك العمليات متعددة ومتلاحقة وأقل من السقف الائتماني للتاجر والذي لا يلزم عنده مراجعة البنك قبل إتمام العملية.

وتكثر تلك الحالات بين أوساط محال بيع المجوهرات والمشغولات الذهبية وشركات السياحة، حيث يوافق هؤلاء التجار أو الباعة على طلب صاحب البطاقة آملاً في أن يقوم بسداد قيمة مشترياته «الوهمية» بالبطاقة لدى عودته إلى بلاده وعدم الاعتراض على تلك العمليات وكثيراً ما يحدث العكس.

أما في الحالة الثانية وهي تورط بعض التجار أو الباعة في عمليات بيع وهمية في غفلة عن صاحب البطاقة فقد سبق أن أوضحنا كيفية حدوث ذلك باستخدام الفواتير والإشعارات مع الختامة اليدوية الخاصة بالتاجر ولكن كثيراً ما يلجأ التاجر أو البائع إلى التلاعب في ماكينات البيع الإلكترونية POS بعد أن يقوم بتحويل مفتاح التحكمSwitch ON/OFF من وضع ON إلى وضع OFF الذي يسمح بإدخال بيانات بطاقات العملاء الذين سبق لهم التردد على المحل في مرات سابقة من خلال لوحة مفاتيح الوحدة دون الحاجة إلى تمرير البطاقة في المسار الخاص بها وإجراء عمليات بيع وهمية ومطالبة البنك بقيمة تلك العمليات فيما بعد، والذي غالباً ما يستجيب بعد خصم قيمة تلك العمليات من رصيد البطاقة من خلال عمليات المقاصة الدولية.

والواقعة هنا أيضاً لا يمكن أن تكتشف إلا في حالة قيام صاحب البطاقة الأصلي بمراجعة كشف الحساب الخاص به بدقة.

وأكثر مرتكبي تلك العمليات هم من الباعة الذين يعملون على وحدات المحاسبة Cashiers في محال الملابس أو الأجهزة الكهربائية أو أدوات التجميل، بعيداً عن أعين أصحاب المحال أو مديريها، حيث يقومون بالاستيلاء على قيمة عمليات البيع النقدية وتحميل قيمة تلك العمليات على بطاقات ائتمان خاصة بآخرين «بالأسلوب السابق» ممن سبق لهم التردد على المحل لشراء بعض السلع باستخدام بطاقاتهم الائتمانية.

٣ . ١ . ٥ تزوير بطاقات الدفع الإلكتروني واستعمالها

ويلزم هنا أن نتعرف على أساليب تأمين البطاقات حتى يمكن التفرقة بين البطاقة الصحيحة والمزورة، وغالبية البطاقات تتفق في معظم عناصر التأمين المتمثلة في[1]:

(١) الباحث، الاحتيالات المصرفية مصدر سابق ص ٢٩.

١ ـ الحروف والأرقام النافرة .
٢ ـ الطباعة الدقيقة .
٣ ـ العلامة ثلاثية الأبعاد «الهولوجرام» .
٤ ـ الطباعة غير الحرفية «تظهر بالأشعة فوق البنفسجية»
٥ ـ صورة العميل[١] .
٦ ـ شريط التوقيع يحمل طباعة أرضية دقيقة بحبر حساس ضد المذيبات والمزيلات الكيميائية .

وتوضح الصور التالية عناصر تأمين كل من بطاقات الفيزا والماستركارد وأميركان إكسبريس .

(١) بعض البنوك والمؤسسات المالية لا تهتم بإضافتها للبطاقة .

وتزوير تلك البطاقات إما أن يكون تزويراً كلياً أو جزئياً .

١ ـ التزوير الكلي

يتم عن طريق اصطناع البطاقة بالكامل وتقليد ما فيها من عناصر تأمين مثل الطباعة البارزة، الطباعة الدقيقة، الشريط الممغنط، وطباعة الـ UV والصورة المجسمة ثلاثية الأبعاد .

٢ ـ التزوير الجزئي

يتم عن طريق استخدام بطاقة صحيحة مسروقة أو مبلغ بفقدها أو منتهية الصلاحية، ثم العبث في بياناتها أو أحد عناصرها التأمينية وبما يسمح باستخدامها بسهولة ودون اعتراض .

٣ ـ ومن الظواهر الدالة على التزوير الكلي للبطاقة:

أ ـ خلو البطاقة من الخواص المميزة للطباعة الدقيقة .

ب ـ رداءة الصورة المجسمة ثلاثية الأبعاد «الهولوجرام» حيث تبدو على أنها صورة لامعة ذات بعد واحد، خالية من الخواص البصرية المميزة لعنصر الهولوجرام .

جـ ـ عدم دقة لصق الشريط الممغنط وشريط التوقيع .

د ـ اختلاف مواصفات وحجم الطباعة البارزة عن نظيرها الصحيح .

هـ ـ خلو البطاقة المقلدة من الطباعة غير المرئية التي تظهر عند تعريضها للأشعة فوق البنفسجية UV .

٤ ـ ومن الظواهر الدالة على التزوير الجزئي للبطاقة

أ ـ ظهور آثار للإزالة الكيميائية للتوقيع في خانة التوقيع .

ب ـ تشوه أو عدم اتساق حواف الصورة المجسمة ثلاثية الأبعاد .

جـ ـ عدم التطابق بين البيانات الملقنة للشريط الممغنط وبين البيانات المقروءة بصرياً .

وفيما يلى بعض نماذج لبطاقات مزورة تزويراً جزئياً

وفيما يلى بعض نماذج لبطاقات مزورة تزويراً كلياً

وأخيراً فإن الدقة والوضوح والانتظام والتناسق والحيوية والخلو من العيوب والتقطعات والتشوهات الطباعية عند فحص سطح البطاقة وما عليها من نقوش وكتابات وعلامات لهو خير دليل على الأرجح على صحة البطاقة.

٢.٣ التطور التكنولوجي وجرائم بطاقات الدفع الإلكتروني

لاحظنا فيما سبق كيف ترك التطور التكنولوجي أثره في تطبيقات واستخدامات بطاقات الدفع الإلكتروني، وكيف تعددت الجرائم المصاحبة لهذا النشاط وتنوعت أساليب ارتكابها، حتى ظهرت أشكال إجرامية جديدة لم تكن معروفة من قبل، اتخذت من بيئة تكنولوجيا المعلومات مناخاً

خصباً، وصعبت مهمة أجهزة المكافحة في مواجهتها في العديد من دول العالم، وهددت صناعة بطاقات الدفع الإلكتروني، وبدأت المنظمات الدولية المعنية مثل فيزا وماستركارد والشركات والهيئات الدولية المنتجة لتكنولوجيا المعلومات في التكاتف مع أجهزة المكافحة المحلية والدولية لمواجهة هذا الخطر الجديد الذي بدا في العديد من صوره على أنه أحد أشكال الجريمة المنظمة عبر الوطنية.

وهذا النوع من الجرائم والذى يدخل ضمن ما يسمى بالجرائم الذكية أو الجرائم عالية التقنية «Hi Technology Crimes» يمكن أن يأخذ أشكالا عديدة، فمنها عمليات اختلاس وسرقة بيانات بطاقات الدفع الاليكتروني وإعادة استخدامها، ومنها ما يرتكب بمعرفة بعض موظفي مراكز البطاقات من ضعاف النفوس، حيث تتيح لهم مهاراتهم الفنية وإلمامهم التام بالبرامج والتطبيقات وعمليات الإصدار والمتابعة وقواعد بيانات عملاء البنك هذه الفرصة، خاصة في ظل وجود بعض الثغرات الفنية والإدارية لدى بعض البنوك.

٣ . ٢ . ١ اختلاس وسرقة بيانات بطاقات الدفع الإلكتروني

عمليات اختلاس أو سرقة بيانات بطاقات الدفع الإلكتروني لها أساليب مختلفة، وتعد من العمليات الفنية المعقدة التي تتطلب ضرورة أن يتوافر لدى مرتكبيها مهارات فنية عالية في تطبيقات الحاسب الآلي المختلفة والاحتراف في التعامل مع شبكة الإنترنت، والأجهزة الإلكترونية الحديثة ومن أهم أساليبها ما يلي:

- تخليق أرقام بطاقات ائتمانية صحيحة Cards Numbers Generating
- نسخ البيانات الملقنة للشريط الممغنط بطريق المغافلة Skimming

ـ السطو الإلكتروني على ماكينات الصرف الآليATMs Fraud

ـ القرصنة عبر شبكة الإنترنت Internet Hacking

ـ رسائل البريد الإلكترونية الخادعة أو ما يعرف بالتصيد Phishing

ونتناول فيما يلي هذه الأساليب بشيء من التفصيل :

١ ـ تخليق أرقام بطاقات ائتمانية صحيحة Cards Numbers Generation

الأصل أن عملية ترقيم البطاقات الصحيحة التي يتم إصدارها داخل مركز البطاقات في أي بنك أو مؤسسة مالية تخضع لمعادلات رياضية معقدة يحكمها شفرة خاصة بكل بنك Algorithm ويتم تحديدها سلفاً بمعرفة كل من المنظمات الدولية المسئولة عن هذا التسلط مثل فيزا وماستر كارد، بحيث يصعب «بل ويستحيل» لأي شخص أن يستنتج بعقله» رقماً لبطاقة من البطاقات الصالحة الصادرة عن أي بنك من البنوك العاملة في هذا النشاط استناداً إلى أرقام صحيحة لبطاقات صادرة عن ذات البنك .

إلا أنه ظهر في نهاية عقد التسعينيات نشاط تخليق أرقام بطاقات ائتمانية صحيحة منسوبة لبعض البنوك عن طريق بعض برامج الحاسب الآلي التي يتم تسويقها من خلال بعض مواقع القرصنة على شبكة الإنترنت .

ويكفي هنا للحصول على برنامج من تلك البرامج أن يتم الدخول إلى أحد تلك المواقع ثم إنزال البرنامج Download إلى الحاسب مقابل مبلغ زهيد من المال وفي المرحلة الثانية تشغيله وإدخال رقم بطاقة ائتمانية صحيحة، ليتولى البرنامج بعد ذلك عملية التخليق Generatingلأرقام بطاقات ائتمانية تصل إلى مائة رقم بطاقة صحيحة منسوبة لذات البنك ثم استخدام تلك الأرقام بعد ذلك في أية عمليات سواء بدمجها مع بطاقات مقلدة أو تلقينها

لأشرطة ممغنطة لبعض البطاقات منتهية الصلاحية واستخدامها في إجراء المعاملات، وبالطبع فإن ناتج هذه العمليات هو خصم قيمتها من الرصيد الائتماني لصاحب البطاقة الأصلية التي تحمل ذات الأرقام والصادرة عن ذات البنك، ودون أن يدري صاحبها، مع الأخذ في الاعتبار أن تلك العمليات لن تكتشف إلا في حالة قيام صاحب البطاقة الأصلية بمراجعة كشف الحساب الوارد من البنك، وهو الأمر الذي كثيراً ما لا يحدث[1].

وأشهر برامج التخليق هو برنامج Card Master.

ويوضح هذا الشكل إحدى صفحات برنامج تخليق أرقام بطاقات الدفع الالكترونى

(١) راجع موقع http://thecreditcardgenerators.com.

٢ ـ نسخ البيانات الملقنة للشريط الممغنط بطريق المغافلة Skimming

انتشرت في السنوات الأخيرة ظاهرة تلقى العديد من البنوك المصرية اعتراضات من بعض أصحاب بطاقات الدفع الإلكتروني Charge Back «من رعايا دول أخرى» على بعض العمليات التي تضمنتها كشوف الحساب الشهرية المرسلة لهؤلاء العملاء حيث أصر أصحاب البطاقات بأن أياً منهم لم يسبق له التردد على هذه البلاد، ولدى قيام الإدارة«بالتنسيق مع مسئولى البنوك» بفحص تلك الاعتراضات، أصر كل من أصحاب المتاجر التي استخدمت فيها تلك البطاقات على صحة وسلامة تلك العمليات التي تمت من خلال وحدة الـ POS الإلكترونية «أي أن البطاقة قد تم تقديمها للتاجر وتم تمرير العملية إليكترونياً من خلال البيانات الملقنة للشريط الممغنط». إلا أنه تبين أن تلك العمليات قد تمت باستخدام بطاقات ائتمانية مزورة إما كلياً أو جزئياً، وأن العديد من التجار في كافة أنحاء العالم قد انخدعوا في تلك البطاقات.

وترجع بداية تلك الظاهرة في النصف الأخير من عقد التسعينيات عندما ابتكر أفراد إحدى الجماعات الإجرامية المنظمة وحدة إلكترونية لنسخ وتخزين البيانات الملقنة للأشرطة الممغنطة Skimmer صغيرة الحجم تعمل بالتيار المتردد ٥ , ١ فولت ويمكن إخفاؤها في الجيب بسهولة. حيث استخدمت تلك الوحدة بمعرفة عاملين في بعض المطاعم والفنادق والمحال العامة في نسخ البيانات الملقنة للأشرطة الممغنطة لبطاقات الائتمان بعد مغافلة أصحابها وحال شروعهم في سداد قيمة مشترياتهم.

وتوضح الصور التالية مراحل تلك العملية:

طباعة الأرقام البارزة مطابقة للبيانات المنسوخة

إعادة تلقين البيانات على بطاقات مزورة تزويرا كليا

نقل بيانات البطاقات على الحاسب

نسخ بيانات البطاقة بعد مغافلة صاحبها بوحدة نسخ صغيرة

ويمكن للوحدة الواحدة التقاط وتخزين بيانات لعشرين بطاقة دفع إليكتروني. وتأتي بعد ذلك المرحلة التالية، حيث يتم تفريغ محتوى هذه الوحدة إلى أحد الملفات على جهاز حاسب آلي ليتم إعادة تلقينها بعد ذلك «من خلال الحاسب الآلي» على أشرطة ممغنطة لبطاقات بلاستيكية خام أو مقلدة أو صحيحة منتهية الصلاحية، باستخدام وحدة تكويد الأشرطة الممغنطة (Encoder)[1].

٣ ـ السطو الإلكتروني على ماكينات الصرف الآلي ATMs Fraud

نظراً لأن عمليات النسخ السابقة سوف لا تمكن محترفي هذا النوع من الجرائم إلا من استخدامها في عمليات الشراء والتسوق فقط، واستحالة استخدامها في عمليات السحب النقدي من خلال آلات الصرف ATM حيث تتطلب العمليات الأخيرة ضرورة إدخال الرقم السري الشخصي PIN personal identification number– لذا فقد ابتكرت بعض العصابات المنظمة

---

(١)راجع مواقع:

http://www.kanecal.net/mag-stripe-
http://stor.aiallc.com.
http://hackershomepage.com.

طرقاً جديدة للسطو الإلكتروني على آلات الصرف الآلي وتمكنوا من خلالها من نسخ بيانات البطاقات الممغنطة التي يتم إيلاجها داخل تلك الماكينات وكذا التقاط الرقم السري الشخصي PIN وذلك باستخدام وحدة نسخ Skimmer يتم تثبيتها بدقة في مكان إيلاج البطاقة داخل الماكينة، وكذا كاميرا تصوير رقمية صغيرة يتم تثبيتها في موضع خفي داخل الصندوق، ترتبط بجهاز إرسال يعمل بالبطارية، إلى شخص مستقبل جالس داخل سيارة بالقرب من موضع ماكينة الصرف الآلي ATM يتولى استقبال تلك الصورة على حاسب آلي نقال لتحديد الأرقام السرية PINs الخاصة بكل من ترددوا على تلك الماكينة لسحب النقود.

ثم يتولى أفراد العصابة بعد ذلك الاستيلاء على تلك البيانات وإعادة تلقينها مرة أخرى إلى بطاقات مزورة واستعمالها في عمليات السحب النقدي مع توافر الأرقام السرية PINs الخاصة بها.

وتوضح الصور التالية مراحل ارتكاب هذا الأسلوب(*).

(*) تم اكتشاف حالات من هذا النوع من الاحتيال فى كل من كندا، الولايات المتحدة الأمريكية، الإمارات العربية المتحدة، هونج كونج وماليزيا، راجع موقعى منظمة الانتربول https://www.interpol.int . و http://www.snopes.com./fraud/atm

٤ ـ القرصنة عبر شبكة الإنترنت Internet Hacking

ويتمثل هذا الأسلوب في لجوء أحد محترفي هذا النوع من الجرائم إلى الدخول إلى شبكة الإنترنت والتنقل بين العديد من مواقع التسوق بحثاً عن المواقع التي لا يتوافر لديها إجراءات حماية و تأمين كافية، ثم يقوم بالولوج إلى تلك المواقع وسرقة بيانات بطاقات الدفع الإلكتروني الخاصة بعملائها.

وهناك العديد من القراصنة Hackers ممن احترفوا إطلاق بعض برامج التلصص عبر الشبكة من خلال المساحات الإعلانية وبعض المواد الدعائية[1]، واستغلالها في التقاط بيانات بطاقات الدفع الإلكتروني الخاصة بمستخدمي الشبكة.

---

(١) وأشهر تلك الأساليب هو الـ Pharming وهو مصطلح لم يكن موجودا فى اللغة الإنجليزية ويشبه فى نطقة كلمة Farming وتعنى الزراعة، وقد أطلق على الطريقة التى يستخدمها صائدو البيانات الشخصية على شبكة الانترنت وتمثل رسائل البريد الاليكترونى الخادعة إحدى أهم وسائل انتشاره حيث تحمل تلك الرسائل برنامج تجسس يتم زرعه على الحاسب الآلى لمتلقي الرسالة بمجرد محاولة فتحها راجع موقع http://en.wikipedia.org.

ويعد هذا الأسلوب من أكثر أساليب اختلاس وسرقة بيانات بطاقات الدفع الإلكتروني انتشاراً، حيث يحترف مرتكبوه اتخاذ كل وسائل التخفي والخداع أثناء ممارسة نشاطهم وبعضهم لا يسعى إلى السرقة بقدر ما يسعى إلى إثبات ذاته وقدرته على اختراق نظم الآخرين.

٥ ـ رسائل البريد الإلكتروني الخادعة Phishing

مصطلح Phishing هو مصطلح حديث لم يكن موجوداً في اللغة الإنجليزية، ولكنه يشبه في نطقه كلمة Fishing التي تعني صيد السمك، وتعتمد هذه الطريقة على خداع المستخدم لكي يبعث بياناته الشخصية والمالية إلى هؤلاء النصابين فيقومون باستخدامها في أنشطة إجرامية أخرى.

والطريقة التقليدية والأكثر شيوعاً في عملية اصطياد البيانات الشخصية والمصرفية تكون عن طريق البريد الإلكتروني. حيث يتلقى المستخدم رسالة إلكترونية من راسل، قد يبدو من الوهلة الأولى أنه بنك أو مؤسسة حكومية أو مالية، تريد أن تتأكد من أن بيانات المستخدم المخزنة لديها هي البيانات الحديثة له، ولذلك عليه أن يعيد إدخال البيانات مرة أخرى في الصفحة التي يوجد عنوانها في الرسالة الإلكترونية. وعنوان الصفحة بتلك الرسالة يكتب بحروف ترمز بالفعل إلى بنك حقيقي أو جهة حكومية أو مؤسسة مالية، ولكن عند الضغط على العنوان بمؤشر الفأرة، يتم تحويل المستخدم إلى موقع آخر على شبكة الإنترنت غير الموقع الذي يظن أنه البنك، هذا الموقع يخص اللص أو القرصان الذي قام بتصميمه، وهو يشبه في الشكل إلى حد كبير صفحة الموقع الأصلي للبنك أو الجهة الحكومية، وعندما يتم إدخال البيانات الشخصية أو المصرفية والضغط على مفتاح إرسال Send أو Submitفإن هذه البيانات تذهب إلى صاحب الموقع الخادع الذي قام

بتصميمه، وقد لا يعلم المستخدم هنا أنه وقع ضحية لعملية احتيال وأن بياناته قد حصل عليها شخص شرير لن يتورع عن استخدامها.

وللأسف فإنه يصعب من النظرة الأولى معرفة ما إذا كانت الرسالة وهمية. وعادة ما يكون أسلوب التعبير في رسائل البريد الإلكتروني لاصطياد الضحايا مهذباً في أغلب الأحوال، ويحاول دائماً دفع المستخدم إلى الرد على الرسالة أو النقر فوق الارتباط المرفق بها، ولزيادة عدد الردود، يحاول المجرمون خلق الشعور بالأهمية ما يدفع الأشخاص إلى الرد الفوري بدون تفكير، وغالباً ماتكون رسائل البريد الإلكتروني شخصية[1] مثل:

عزيزي عميل البنك الهام، لقد بلغنا أنه يجب تحديث معلومات حسابك نظراً لوجود تقارير حول عملية احتيال وانتحال هوية لعضو غير نشط وفي حالة الإخفاق في تحديث السجلات الخاصة بك فسوف يتم إلغاء حسابك، الرجاء اتباع الارتباط أدناه لتأكيد بياناتك.

وعادة ما تركز الرسائل الخادعة على البيانات التالية:

اسم العميل كاملاً:

رقم التأمين الاجتماعي أو الرقم القومي:

رقم حساب البنك:

رقم بطاقة الصراف الآلي ATM:

رقم بطاقة الائتمان أو الخصم Credit Card أو Debit Card

كلمة المرور أو رقم التعريف PIN

(١) راجع موقع شركة مايكروسوفت والتعرف على خدع البريد الإليكتروني الوهمية واصطياد الضحايا http://office.microsoft.com

عنوان البريد الإلكتروني

الاسم المدون على بطاقة الائتمان

قيمة التحقق من(*) البطاقة Card verification Value - CVV2

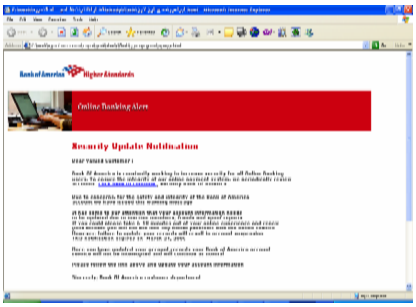
تاريخ الميلاد :

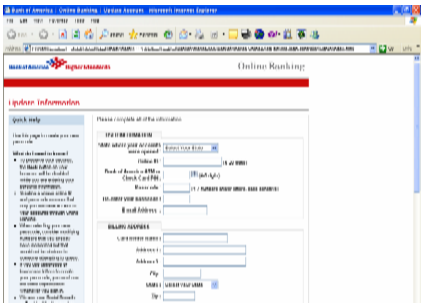
العنوان :

رقم تليفون العمل والمنزل :

رقم رخصة القيادة :

رسالة تصيد مكونة من صفحتين منسوبة لبنك أوف أمريكا





ويرجع تاريخ أول حالة تصيد Phishing عبر شبكة الإنترنت عن طريق الرسائل الإلكترونية الخادعة إلى أكتوبر عام ٢٠٠١ عندما قام أحد الأشخاص ببث عدة آلاف من الرسائل الإلكترونية الخادعة عبر شبكة الإنترنت مستهدفاً عملاء أحد أكبر المتاجر الإلكترونية عبر شبكة الإنترنت

(*) وهو رقم مكون من ثلاث خانات يتم طبعه على ظهر البطاقة ، ويطلب من حاملها فقط في حالة طلب الخدمات المسموح بتقديمها وسداد قيمتها من خلال التليفون أو البريد الإليكتروني ، للتأكد من أن البطاقة في يد الطالب حال طلبه للخدمة .

وهو epay وقام بشراء أجهزة إلكترونية وحاسبات آلية نقالة باستخدام أرقام وبيانات بطاقات الائتمان التي حصل عليها، وقام بإجراء تحويلات نقدية عن طريق مؤسسة وسترن يونيون إلى حساب قام بفتحه في أحد البنوك بمدينة لوس أنجلوس الأمريكية ثم قام بتحويلها بعد ذلك إلى حسابين بنكيين في كل من لتوانيا وأوكرانيا وقد قامت الشرطة الملكية التايلاندية بضبطه بتاريخ ٢١/ مايو عام ٢٠٠٣ وتبين أنه يدعى ماكسيم كوكلاك روسي الجنسية[١].

ويشير أحدث تقارير شركة سيمانتيك Symantec إلى أن تهديدات التصيد الاحتيالي Phishing قد زادت بصورة كبيرة خلال السنوات الأخيرة، حتى إنه تم رصد ٩ , ٧ مليون محاولة يومياً لتصيد البيانات خلال النصف الأخير لعام ٢٠٠٥[٢].

وقد كشفت الدراسة وما تم ضبطه من قضايا عن أن ضحايا هذا النوع من الجرائم الـ Phishing يتمركزون في الدول المتقدمة خاصة الولايات المتحدة الأمريكية وغرب أوروبا حيث يزداد اعتماد المواطنين على الخدمات المصرفية الإلكترونية بصفة يومية، أما مرتكبوها فيتمركزون في الدول النامية أو الأقل أخذاً بأسباب التقدم التكنولوجي، وذلك لضعف الاعتماد على الخدمات المصرفية الإلكترونية، وأيضاً لضعف وعدم كفاءة أجهزة المكافحة في تلك الدول.

---

(١) راجع موقع http://www.usdoj.gov/usao/cmn/press

(٢) شركة سيمانتيك Symantec هي من أكبر الشركات العالمية المتخصصة في أمن المعلومات والشبكات، وتقوم بإصدار تقارير متابعة دورية عن تلك الأنشطة، راجع موقع http://www.symantec.com

ويمكن بعد اختلاس وسرقة بيانات بطاقات الدفع الإلكتروني استخدامها فيما يلي :

١ ـ تلقين تلك البيانات «المسروقة» للأشرطة الممغنطة الخاصة ببطاقات منتهية الصلاحية باستخدام وحدة تكويد Encoder تزوير جزئي، أو تلقينها لبطاقات بلاستيكية خام وطباعة بيانات لبنوك حقيقية أو وهمية عليها من الخارج، لتبدو وكأنها بطاقات دفع صحيحة «التزوير الكلي» .

٢ ـ استخدام البيانات «المسروقة» في تمويل عمليات شراء أو تسوق من خلال شبكة الإنترنت .

٣ـ الاتجار في البيانات المسروقة أو تبادلها مع آخرين من خلال المنتديات الخاصة Chatting Rooms عبر شبكة الإنترنت .

٦ ـ جرائم موظفي مراكز البطاقات

تعد مراكز البطاقات لدى البنوك بمثابة مراكز لشبكات معلومات كل من حاملى البطاقات والتجار وتخضع عمليات إدارة وتشغيل تلك الشبكات لمعايير فنية دقيقة تفرضها العلاقة التعاقدية بين كل من البنك والمنظمات الدولية مثل فيزا Visa ماستركارد Master Card .

وتعد الثغرات الفنية والإدارية في عمليات تشغيل وإدارة تلك الشبكات هى المدخل الرئيسى لمرتكبى هذا النوع من الجرائم من بعض موظفي تلك المراكز، خاصة في ظل عدم قيام العديد من حاملى البطاقات والتجار بمراعاة الدقة في مراجعة كشوف الحسابات الواردة إليهم من البنك .

وهناك العديد من الأمثلة على ذلك، سوف نعرض لبعضها في الجانب التطبيقى من هذه الدراسة، منها ذلك الموظف الذى كان يعمل في قسم صيانة وحدات البيع الاليكترونية لدى التجار « POS» الذى استغل وجود ثغرات فنية في نظام البنك وقام بمغافلة البائع وأجرى عمليات ارتجاع وهمية لبعض السلع على وحدة الـ «POS» راداً قيمتها إلى حساب رقمي بطاقتي فيزا تبين أن أحداهما باسمه والاخري لصديقه.

وآخر يعمل في قسم الصيانة أيضا، قام أثناء عمل صيانة لوحدة الـ «POS» في أحد مطاعم فندق شهير بتكويد تلك الوحدة ببيانات وحدة أخرى لدى محل ملابس صغير بأحد المراكز التجارية، كان من نتيجة ذلك أن ذهبت حصيلة المبالغ التي سددها المترددون على المطعم إلى حساب صاحبة محل الملابس.

وثالث كان يعمل بقسم طباعة وإصدار البطاقات لدى أحد البنوك الكبرى، كان يقوم بطباعة صورته الشخصية على بطاقات تحمل بيانات عملاء البنك من أصحاب البطاقات المرتدة من الفروع لعدم استلامها

ويجب هنا الإشارة إلى أن البنوك يجب أن تلتزم بتطبيق المعايير التي تفرضها المنظمات الدولية مثل فيزا Visa، ماستركارد Master Card بشأن إجراءات الرقابة داخل مراكز البطاقات، وبما يضمن الحفاظ على الأمن وسرية المعلومات التي تحويها تلك المراكز[1].

---

(١) راجع فاليري عساف، مسئول الأخطار بمنظمة الفيزا العالمية ورقة عمل بشأن إجراءات ومعايير الرقابة داخل مراكز البطاقات، منتدى مكافحة الاحتيال الربع سنوي، مكتب منظمة الفيزا بالقاهرة، ديسمبر ٢٠٠٦.

٣ .٣ الخسائر المادية والمردودات السلبية

إذا كنا قد تناولنا في المبحث الأول الأنماط المختلفة لجرائم بطاقات الدفع الإلكتروني وأثر التطور التكنولوجي على هذا النوع من الجرائم في المبحث الثانى ، إلا أن هناك العديد من التساؤلات التي تفرض نفسها في هذه المرحلة من الدراسة ألا وهي :

- من الذي يتحمل الخسارة المادية ؟ هل هو حامل البطاقة ؟ أم التاجر ؟ أم البنك؟
- هل يمكن تحديد حجم الخسائر؟
- وما الآثار السلبية المترتبة على هذا النوع من الجرائم؟ .

والإجابة على هذه الأسئلة تتضمنها «في غالب الأحيان » بنود التعاقد بين البنك وحامل البطاقة أو بين البنك والتاجر بالإضافة لنظم وقواعد المنظمات الدولية مثل فيزا وماستر كارد، ولتحديد مسئولية أي طرف من الأطراف الأربعة «التاجر، بنك التاجر، حامل البطاقة، البنك المصدر» في تحمل الخسارة في حالة وجود عمليات غير سليمة نتيجة ارتكاب أحد الأنماط الإجرامية السابق الإشارة إليها، يتعين علينا أولا تحديد أنواع الحركات التي تتم باستخدام هذا النوع من البطاقات على النحو التالي :

٣ .٣ .١ حركات لا تقدم فيها البطاقات Card-not- present Transactions

وهى الحركات التي لا تستلزم وجود بطاقات أثناء العملية، مثل تلك التي تتم من خلال التليفون أو البريد الإلكتروني، وفي هذه الحالة تقع الخسارة على التاجر وبنك التاجر في حالة عجز التاجر عن إثبات أن الحركة تمت بمعرفة العميل، حيث إن كافة الحركات التي لا تقدم فيها البطاقات

يجب أن يدون التاجر مع رقم البطاقة الكود التأميني المعروف باسم CVV2 وهو مكون من ثلاثة أرقام مطبوع بجانب رقم البطاقة المطبوع على ظهر البطاقة، حيث يقوم صاحبها بإملائه للتاجر الذى يتعامل معه من خلال التليفون أو البريد الاليكتروني، دلالة على أن البطاقة في يد صاحبها عند طلب أمر الشراء.

وفي كثير من الأحيان يقوم التاجر بإرفاق صورة ضوئية من البطاقة أو صورة تحقيق الشخصية لصاحبها وكلها قرائن تفيد أن العملية قد تمت بمعرفة الأخير.

لذا فإنه في حالة عجز التاجر عن تقديم ما يفيد إتمام الحركة بمعرفة العميل يكون الفيصل في تحديد المسئولية هو العقد الذى يربطه بالبنك وما يتضمنه من شروط لصحة إتمام العمليات وتحديد مسئولية التاجر، وغالبا ما تشترط البنوك في مثل هذه العقود أن يتحمل التاجر المسموح له بالتعامل بهذا النظام الخسارة كاملة في حالة ارتداد الحركات[1].

٣ .٣ .٢ الحركات التي تستلزم تقديم البطاقات

وهذه النوعية من الحركات تكون لها إشعارات خصم تثبت فيها أن البطاقة كانت متواجدة أثناء العملية وذلك على النحو التالي:

١ ـ العمليات اليدوية

وهى العمليات التي يحصل فيها التاجر على بصمة البطاقة البارزة «أثناء إجراء عملية الشراء» على إشعارات «ذات خاصية كربونية»، وهى دليل

(١) فهيم كامل فهيم، المرجع العلمي لأعمال ادارة أخطار بطاقات الائتمان، البنك الأهلى المصري، قطاع بطاقات الائتمان والتجزئة المصرفية، ص ٣٠.

قاطع على أن البطاقة كانت متواجدة أثناء العملية، وعليه لا يمكن رد المبلغ أو قبول اعتراض صاحب البطاقة على العملية.

وفي حالات سرقة بصمة البطاقة «عن طريق المغافلة» على إشعار خال واستكمال الحركة وخصمها عن طريق البنك، بالطبع فإن قيمة هذه العملية يتحملها صاحب البطاقة، أما إذا اعترض عليها وتمكن هو أو السلطة المختصة « من إثبات عدم قيامه بهذه الحركة مثل اعتراض بعض السائحين على عمليات تمت من خلال إشعارات يدوية بعد مغادرتهم للبلاد» فتقع الخسارة على التاجر، وهناك العديد من القرائن الأخرى التي يمكن الاستناد إليها في مثل تلك الحالات.

٢ ـ الحركات الالكترونية

وتتميز الماكينات الاليكترونية بخاصية قراءة البيانات الملقنة للشريط الممغنط وتظهر تلك البيانات على الاشعارات الصادرة عن الماكينة كما تسجل الحركة لدى مركز معلومات البنك وكذا مركز معلومات الهيئة أو المؤسسة الدولية سواء أكانت فيزا أو ماستركارد أو أمريكان اكسبريس.

لذا فإنه في حالات التزوير الشهيرة والمعروفة باسم النسخ أو Skimming، فتقع الخسارة كاملة على البنك المصدر للبطاقة، نظرا لأن الشريط الممغنط قد تمت قراءته، ويحتدم النزاع بين البنك المصدر وحاملى البطاقات، وغالباً ما يتحمل البنك الخسارة في حالات التزوير الجماعية كما حدث في حالة بلاغ انتربول كانبرا باستراليا.

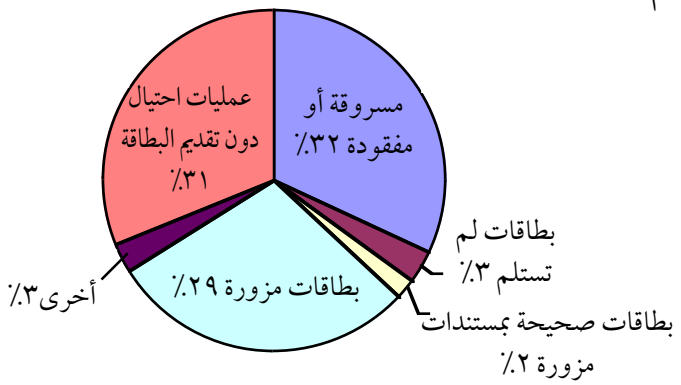
وفي حالة التصيد المعروفة باسم Phishing فان الخسارة تقع على حامل البطاقة بالطبع في كافة العمليات التي يقوم المحتالون بأدائها باستخدام أرقام البطاقة التي تصيدوها.

وكما سبق أن أوضحنا فإنه يصعب الحصول على إحصاءات دقيقة عن حجم العمليات التي يتم إجراؤها باستخدام كافة أنواع بطاقات الدفع الالكترونية حول العالم، وقد زاد الأمر تعقيدا لدى محاولة الحصول على إحصاءات دقيقة بشأن حجم الخسائر وتصنيفها، نظراً لاحتدام المنافسة بين الهيئات والمؤسسات المصدرة أو المسئولة عن تلك البطاقات مثل فيزا، ماستر كارد، أمريكان اكسبريس.

إلا أنه أمكن الحصول على بعض الإحصاءات الخاصة بمنظمة الفيزا العالمية، ونظراً لأن عمليات منظمة الفيزا العالمية تمثل حوالى نسبة ٦٠٪ من حجم العمليات على مستوى العالم[١]. فإنه يمكن اتخاذ تلك الأرقام كمؤشر عام.

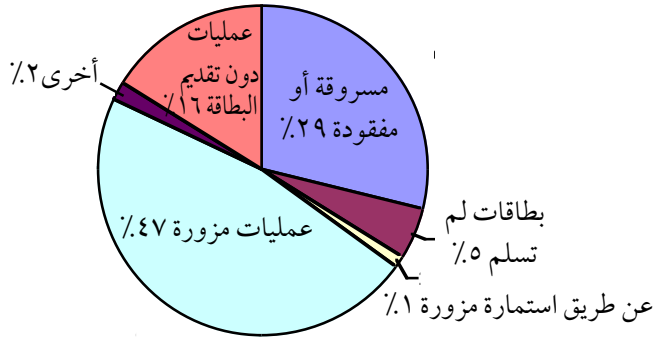
ويشير آخر إحصاء تحليلي لمنظمة الفيزا العالمية إلى أن حجم الخسائر على مستوى العالم قد بلغ عام ٢٠٠٥ م حوالى ٢,٢ مليار دولار أمريكى

ويوضح الرسم التالي مقارنة بين أنواع جرائم البطاقات على مستوى العالم.



(١) وفقا لتقرير نيلسون لعام ٢٠٠٦م، مرجع سابق.

ويوضح الرسم التالي مقارنة بين أنواع الاحيتال في منطقة وسط وشرق أوروبا والشرق الأوسط وإفريقيا[١]:



كما يوضح البيان التالي حالات احتيال التجار التي تم الإبلاغ عنها في جمهورية مصر العربية عام ٢٠٠٥م والدول التي تعرض رعاياها للاحتيال مرتبة بحسب حجم المبالغ والحالات[٢].

البلد	الكمية	العدد	المعدل	النسبة
الولايات المتحدة الأمريكية	٩٧,٦٩٣	٢٢٤	$٤٣٦	٣٦,٤٦٪
المملكة المتحدة	٥٧,٤٩١	٩٧	$٥٩٣	٢١,٤٥٪
مصر	٢١,٠٠٨	١٢٠	$٤٧٥	٧,٨٤٪
كندا	١٩,٢٠٦	١٠	$١,٩٢١	٧,١٧٪
اليابان	١٤,١٨٢	١٠	$١,٤١٨	٥,٢٩٪
فرنسا	١٢,٠٨٦	٣٦	$٣٣٦	٤,٥١٪
سويسرا	٩,٢٩٢	٦	$١,٥٤٩	٣,٤٧٪
ايطاليا	٨,٩١٧	٢٧	$٣٣٠	٣,٣٣٪
المملكة العربية السعودية	٨,٣٨١	٤٣	$١٩٥	٣,١٣٪
ألمانيا	٧,٠٠٣	٣٠	$٢٣٣	٢,٦١٪
أفضل ١٠ بلدان	٢٥٥,٢٥٨	٦٠٣	$٤٢٣	٩٥,٢٥٪
كل البلدان الأخرى	١٢,٧٢٢	٥٨	$٢١٩	٤,٧٥٪
الإجمالى	٢٦٧,٩٨٠	٦٦١	$٤٠٥	١٠٠٪

(١) تقوم الهيئات والمنظمات الدولية بتقسيم العالم جغرافيا الى ٦ مناطق هى آسيا والباسفيك، الولايات المتحدة الأمريكية، كندا، أمريكا اللاتينية، أوروبا، شرق أوروبا والشرق الأوسط وإفريقيا.

(٢) مصدر هذا البيان، مكتب منظمة الفيزا العالمية بالقاهرة.

ويوضح البيان التالي حجم وعدد الحالات التي تم الإبلاغ عنها لبطاقات صادرة من بنوك مصرية تعرض أصحابها للاحتيال من خلال تجار في العديد من دول العالم خلال عام ٢٠٠٥م مرتبة حسب حجم تلك الحالات وعددها :

البلد	الكمية	العدد	المعدل	النسبة
ايطاليا	٣١,٩٧٦	١٠١	$٣١٧	٪٢٧,٥١
مصر	٢١,٠٠٨	١٢٠	$١٧٥	٪١٨,٠٨
المملكة المتحدة	١٤,٤٧٧	٣٣	$٤٣٩	٪١٢,٤٦
تركيا	٨,٥٣٢	٢٦	$٣٢٨	٪٧,٣٤
ألمانيا	٧,٦١٣	١٦	$٤٧٦	٪٦,٥٥
المملكة العربية السعودية	٦,٥١٦	٢٧	$٢٤١	٪٥,٦١
فرنسا	٤,٨٣٢	٢٨	$١٧٣	٪٤,١٦
الولايات المتحدة الأمريكية	٤,٠٠٨	٧٠	$٥٧	٪٣,٤٥
تايلاند	٢,٦١٧	١٥	$١٧٤	٪٢,٢٥
استراليا	٢,٥١٥	٤	$٦٢٩	٪٢,١٦
أفضل ١٠ بلدان	١٠٤,٠٩٥	٤٤٠	$٢٣٧	٪٨٩,٥٧
كل البلدان الأخرى	١٢,١٢١	١٥٣	$٧٩	٪١٠,٤٣
الإجمالى	١١٦,٢١٦	٥٩٣	$١٩٦	٪١٠٠

وأخيرا وليس آخراً هل هناك مردودات سلبية من جراء انتشار هذا النوع من الجرائم ؟

بالطبع هناك الكثير من تلك الآثار التي تتمثل فيما يلى :

١ ـ إحجام العديد من المواطنين ممن وقعوا ضحايا لهذا النوع من الجرائم من الإقبال عليها أو استعمالها في تلبية احتياجاتهم اليومية ، فضلا عن عزوف باقى المواطنين عن الإقبال عليها ، الأمر الذى قد يضعف من فرص نشرها وما يترتب على ذلك من حرمان المواطنين من مزاياها .

٢ـ الآثار السلبية على سمعة السياحة في أي دولة يرتكب بعض رعاياها هذا النوع من الجرائم، ما قد يدفع بعض السائحين من الضحايا إلى الإحجام عن زيارة هذه البلاد مرة أخرى.

٣ـ قد تتعرض بعض البنوك للآثار السلبية لهذا النوع من الجرائم من جراء ضبط بعض موظفيها لتورطهم في وقائع مرتبطة بعملهم في مراكز البطاقات، وهو ما قد يدفع عملاءها إلى التوقف عن التعامل مع البنك، أو الاعتراض على عمليات صحيحة بدون وجه حق بزعم أنها تدخل ضمن ما تم كشفه من وقائع.

٤ـ اهتزاز ثقة المواطنين في القطاع المصرفي عند تكرار نشر تلك الوقائع في الصحف ووسائل الإعلام.

الفصل الرابع

مواجهة جرائم بطاقات الدفع الإلكتروني

٤ .مواجهة جرائم بطاقات الدفع الإلكتروني

سبق أن أوضحنا أن هذا النوع من الجرائم يتميز بطبيعة خاصة، يغلب عليها الطابع الفنى والتقنى، لارتباطها ببعض تطبيقات الحاسب الآلي ونظم الاتصالات، كما أن مرتكبيها على درجة عالية من الوعى والثقافة والذكاء، لذا فإن مواجهة تلك الجرائم يجب أن تتم من خلال منظومة متكاملة تستند إلى دعامات عديدة :

دعامة تشريعية : وتعني وجود تشريع عقابى صريح ورادع لمرتكبى هذا النوع من الجرائم.

دعامة أمنية : وتعني وجود جهاز أمني قادر على مواجهة هذا النوع من الجرائم ومتابعة إفرازات التكنولوجيا الحديثة ويتمتع بالكفاءة والتدريب المستمر.

الجهود الدولية : وتعني وجود أسس دولية لتعزيز التعاون الدولي بين أجهزة المكافحة المعنية بمواجهة هذا النوع من الجرائم في الدول المختلفة.

ولا يجب أن تعتمد مواجهة هذا النوع من الجرائم على الجهود الحكومية فقط، بل إن هناك حلولاً فنية تقدم بمعرفة المنظمات الدولية المعنية بإصدار هذا النوع من البطاقات وكذا البنوك والتجار، وهناك أخيرا محاذير يجب التحوط لها ونصائح يجب على حاملي البطاقات اتباعها.

لذا فإننا سنتناول هذه الدعامات بشئ من التفصيل من خلال مباحث ثلاثة فنتحدث في المبحث الأول عن المواجهة التشريعية، ونتحدث في المبحث الثانى عن كيفية مواجهة هذا النوع من الجرائم من الناحية الأمنية

وكذا الجهود الدولية التي يتم بذلها في هذا المجال، بينما نتحدث في المبحث الثالث عن الحلول الفنية على مستوى المنظمات المعنية بإصدار هذا النوع من البطاقات وكذا البنوك والتجار والأفراد.

٤ .١ المواجهة التشريعية لجرائم بطاقات الدفع الإلكتروني

استعرضنا في الفصل السابق الأنماط الإجرامية المختلفة لجرائم بطاقات الدفع الاليكتروني، وإذا أمعنا النظر في تلك الأنماط سوف نجد أنها تعكس أفعالا غير مشروعة يمكن تقسيمها إلى فئتين

١ ـ أفعال «غير مشروعة» محكومة بعلاقة تعاقدية محددة سلفاً سواء أكانت تلك العلاقة بين حامل البطاقة والبنك المصدر لها، أو بين التاجر والبنك المتعاقد معه لتحصيل قيم مبيعاته بالبطاقات

٢ ـ وأفعال أخرى «غير مشروعة» تخرج عن حدود العلاقة التعاقدية وتشكل انتهاكا صارخاً لحقوق الآخرين، كالبنوك والمؤسسات المالية والتجار والأفراد.

فضلاً عن أن جانباً كبيرا من تلك الأفعال «بفئتيها» بات يرتكب من خلال تطبيقات مختلفة للحاسب الآلي، تشكل في حد ذاتها انتهاكاً للخصوصية وحقوق المجتمع والآخرين .

وقد أثارت جرائم بطاقات الدفع الاليكتروني، ومعها جرائم نظم المعلومات تحديات جساماً في النظام القانونى, وعلى الأخص بالنسبة لقانون العقوبات، ويرجع السبب في ذلك إلى أن القوانين العقابية كانت إلى وقت قريب تبسط حمايتها على الأشياء المادية والمرئية، أما بالنسبة للمعلومات

والقيم المعنوية الأخرى المرتبطة بها، التي ظهرت في النصف الثانى من القرن الماضي، فلم تمتد إليها هذه الحماية إلا في حدود ضيقة[1].

وهناك العديد من التشريعات التي تضمنت نصوصا خاصة بهذا النوع من الجرائم، ظهرت في السنوات العشر الأخيرة « خاصة في العديد من دول العالم المتقدم» إلا أنها عالجت الأفعال غير المشروعة التي تمثل انتهاكا لحقوق الآخرين، تاركة الأفعال الأخرى» المحكومة بالعلاقة التعاقدية استناداً إلى قاعدة أن العقد شريعة المتعاقدين.

بينما خلت تشريعات العديد من الدول خاصة الدول النامية « ومنها أغلب الدول العربية » من أية نصوص تجرم تلك الأفعال، تاركة الأمر لاجتهاد القضاء، استناداً إلى نصوص المواد العقابية المتعلقة بالسرقة والاحتيال والتزوير.

ونستعرض فيما يلي موقف بعض التشريعات الجنائية على المستويين الدولى والعربى.

٤ .١ .١موقف بعض التشريعات الجنائية على المستوي الدولى

١ ـ الولايات المتحدة الأمريكية : تتضمن المادة ١٨ من قانون العقوبات الفيدرالي النص على تجريم كافة الأفعال المصاحبة لنشاط بطاقات الدفع الاليكتروني وتشمل الاستخدام غير المصرح به، سرقة البطاقات واستخدامها، استخدام البطاقات المفقودة، والمنتهية الصلاحية أو الملغاة، والاتجار في البطاقات غير المصرح باستخدامها وتقليد البطاقات وتزويرها واستعمالها مع العلم بذلك.

---

(١) محمد سامى الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ، القاهرة، ط ٢ ، ١٩٩٨م، ص ٢٣١ . .

وقد توسع نص هذه المادة فشمل وسائل السداد الاليكتروني الأخرى، كما قامت بتجريم حيازة الأجهزة والأدوات التي تساعد على تقليد وتزوير البطاقات متى كان ذلك بقصد غير مشروع.

كما قام المشرع الأمريكي في ٢٨ فبراير ٢٠٠٥م بإضافة فقرة إلى نص هذه المادة لتجريم كافة أعمال التصيد الاحتيالى، فيما سمي بقانون مواجهة التصيد الاحتيالي Aniti- phishingAct of 2005 [١] والتي تعاقب مرتكبي عمليات اختلاس وسرقة بيانات وأرقام بطاقات الدفع الاليكتروني وبطاقات الهوية والحسابات البنكية بالسجن لمدة خمس سنوات.

٢ـ سويسرا: تجرم المادة ١٤٨ من قانون العقوبات السويسري منذ عام ١٩٩٥م العديد من الأفعال المصاحبة لنشاط بطاقات الدفع الاليكتروني التي من شأنها إحداث ضرر بالغير، وقد توسع نص هذه المادة في تحديد البطاقة التي يشملها التجريم حيث نص على عبارة «أو أية وسيلة مماثلة للوفاء» لتشمل بذلك البطاقات التي يتم إصدارها من قبل بعض المتاجر والمحلات التجارية لزبائنها للوفاء بواسطتها[٢].

٣ـ إيطاليا: نصت المادة ١٢ من القانون ٧٢ لسنة ١٩٩٢م على أن يعاقب كل من يسيئ استخدام بطاقة ائتمان أو بطاقة مدنية أو ما شابهها من وسائل السداد إذا ما استخدمها بغرض سلب الأموال

---

(١) راجع النص الكامل لفقرات المادة ١٨ وتعديلها بالقانون الصادر عام ٢٠٠٥ على موقع مكتبة الكونجرس الأمريكي http://www.gotrack.us/congress.

(٢) سامح محمد عبد الحكم، الحماية الجنائية لبطاقات الائتمان، دار النهضة العربية، القاهرة ٢٠٠٣ م، ص ١٣٠ وما بعدها.

رغم انه ليس بمالكها الشرعى، أو قام باستعمالها في السداد النقدي المقدم أو في سداد قيمة بضائع أو خدمات بالسجن من عام إلى خمسة أعوام أو الغرامة التي تتراوح بين ٦٠٠ ألف و٣ ملايين ليرة إيطالية[١]، وتنطبق ذات العقوبة على كل من زيف جزئيا أو كليا بغرض الاستيلاء على المال بطاقات ائتمان أو بطاقات مدنية أو ما شابهها من وسائل السداد، مستغلاً إياها في السداد النقدي المقدم، أو في سداد قيمة بضائع أو خدمات، وكذا كل من باع أو اشترى مثل هذه البطاقات أو الوسائل ذات الأصل غير المشروع سواء أكان تزييفها كلياً أو جزئياً وينطبق العقاب على مروج حوالات السداد المطبوعة.

٤ ـ فلندا : تعاقب المادة الثامنة من الفصل السابع عشر من قانون العقوبات، كل من يقوم لأجل الحصول على ربح أو عائد مالي بدون وجه حق له أو للغير سواء باستعمال بطاقة بنكية أو ائتمانية أو شيك أو أية وسيلة سداد مشابهة دون موافقة مالكها الاصلي متجاوزا الحقوق المكفولة له، أو دون حق شرعى أو دون تصريح من الجهة المانحة للبطاقة أو بالتجاوز للتصريح الممنوح من تلك الجهة، وكذلك بنقل هذه البطاقة للغير لاستخدامها دون أن يكون له الحق قانوناً في ذلك، ويشير نص المادة صراحة إلى الحالات التي يتم الاستخدام غير الشرعى للبطاقة فيها مثل سحب ما يجاوز الرصيد أو ما يجاوز الحد الأقصى المسموح به، كما عاقبت المادة التاسعة من ذات القانون مرتكب إنتاج أو تقليد وسائل السداد المزيفة باعتبارها جريمة احتيال.

---

(١) تم تعديل قيمة هذه الغرامة إلى عملة اليورو الأوروبي.

٥ ـ فرنسا : نص المشرع على حماية جنائية خاصة لبطاقات الدفع الاليكتروني بالقانون رقم ١٣٨٢ الصادر في ٣٠ ديسمبر ١٩٩١م بإضافة فقرتين إلى المادة ٦٧ من قانون العقوبات الفرنسي، حيث تنص الفقرة الأولى منه على معاقبة كل من زيف أو عدل إحدى بطاقات السداد، وكل من استخدم أو حاول استخدام بطاقة سداد أو بطاقة مدنية تم تزييفها أو تعديلها مع علمه بذلك، كذلك كل من اتفق على استلام مستحقات عن طريق بطاقة سداد تم تزييفها أو تعديلها مع علمه بذلك يعاقب بالسجن من سنة إلى خمس سنوات وبغرامة من ٢٠٠٠٠ فرنك إلى ٢٠٠٠٠٠ فرنك، أما الفقرة الثانية فقد نصت على أنه يتعين في الجرائم السابقة مصادرة البطاقات، أو الأدوات المعدة أو المستخدمة في التزوير والتقليد، إلا إذا استخدمت بدون علم مالكها[1].

وقد كان المشرع الفرنسي سباقاً بتجريم الأفعال المرتبطة بنظم المعلومات وتطبيقات الحاسب الآلي وذلك بالقانون الصادر في ٥ يناير ١٩٨٨ بموجب المادة ٤٦٢ والمسمى بقانون الغش المعلوماتي أو قانون البيانات المعالجة إليكترونياً ، والذي يطبق حالياً على جانب كبير من جرائم بطاقات الدفع الاليكتروني المرتبطة بتكنولوجيا المعلومات التي انتشرت مؤخرا على المستوى الدولي.

---

(١) سامح محمد عبد الكريم، الحماية الجنائية لبطاقات الائتمان، مرجع سابق، ص ١٣٢.

٤ .١ .٢ موقف التشريعات الجنائية في بعض الدول العربية

خلت التشريعات العقابية لمعظم البلدان العربية من أية نصوص صريحة تجرم الأفعال غير المشروعة المصاحبة لنشاط بطاقات الدفع الاليكتروني اكتفاء بنصوص المواد العقابية المتعلقة بجرائم السرقة والتزوير والاحتيال وخيانة الأمانة.

وبرغم أن الأعوام القليلة الماضية قد شهدت صدور قوانين لتنظيم المعاملات الالكترونية في بعض الدول العربية[1]، إلا أن نصوص هذه القوانين لم تتعرض لهذا النوع من الجرائم، سوى بتجريم بعض الأفعال المرتبطة بهذا النشاط، بينما تضمن قانون العقوبات في كل من قطر وسلطنة عمان نصوصاً واضحة تجرم بعض تلك الأفعال صراحة.

ونعرض فيما يلي موقف المشرع الجنائي في كل من الأردن، البحرين، سلطنة عمان، قطر، والمغرب، إمارة دبى.

١ ـ الأردن : لم يتعرض المشرع لنصوص عقابية صريحة تجرم الأفعال غير المشروعة المصاحبة لنشاط بطاقات الدفع الاليكتروني تاركاً الأمر للقضاء استناداً إلى نصوص قانون العقوبات المتعلقة بجرائم السرقة والنصب والتزوير.

---

(١) قامت لجنة الأمم المتحدة للقانون التجاري الدولى Uncitral، باعداد القانون النموذجي للتجارة الاليكترونية الذي تم إقراره بمعرفة الجمعية العامة بتاريخ ١٦ ديسمبر ١٩٩٦م، وكذا قانون الاونسترال النموذجي بشأن التوقيعات الاليكترونية والذى تم إقراره بمعرفة الجمعية العامة فى٥ يوليو ٢٠٠١م، وقد قام العديد من دول العالم بالاسترشاد بهذين النموذجين في استصدار القوانين اللازمة لتنظيم أعمال التجارة والمبادلات الإلكترونية كان من بينها كل من الأردن، تونس، البحرين، مصر، دبي، راجع النصوص كاملة لتلك القوانين على موقع حكوميات http://www.egovs.com

بينما تضمن قانون المعاملات الإلكترونية رقم ٨٥ الصادر بتاريخ ١١ ديسمبر سنة ٢٠٠١ م في المادة ٣٥ منه بأن يعاقب كل من يقوم بإنشاء أو نشر أو تقديم شهادة توثيق لغرض احتيالى أو لأي غرض غير مشروع بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين أو بغرامة لا تقل عن ٣٠٠٠ ثلاثة آلاف دينار ولا تزيد على ١٠٠٠٠ عشرة آلاف دينار أو بكلتا هاتين العقوبتين.

كما نصت المادة ٣٨ بأن يعاقب كل من يرتكب فعلاً يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الاليكترونية بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن ٣٠٠٠ ثلاثة آلاف دينار ولا تزيد على ١٠٠٠٠ عشرة آلاف دينار أو بكلتا هاتين العقوبتين، ويعاقب بالعقوبة الأشد إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذا القانون[1].

٢ ـ البحرين : أيضاً لم يتعرض المشرع البحريني لنصوص عقابية واضحة وصريحة تجرم الأفعال غير المشروعة المصاحبة لنشاط بطاقات الدفع الإليكترونى، شأن غالبية الدول العربية إلا أن المادة ٢٤ من قانون التجارة الاليكترونية الصادر بتاريخ ١٤ سبتمبر ٢٠٠٢م تضمنت أنه يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تتجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من ارتكب عمداً فعلا من الأفعال التي وردت على سبيل الحصر بشأن نسخ أو حيازة أو تحريف أو تغيير أو استعمال أو إفشاء شهادة

(١) راجع التشريعات الأردنية على موقع نظام المعلومات الوطني الأردني http:www.lob.gov.go/ui/laws.

أو توقيع إلكتروني لغرض احتيالي أو لأي غرض غير مشروع، أو انتحال هوية شخص آخر في طلب الحصول على شهادة أو تعديلها.

٣ـ سلطنة عمان: تضمن التشريع العقابي العماني النص على عقوبات لغالبية الأفعال غير المشروعة في مجالي استخدامات الحاسب الآلي وبطاقات الدفع الإليكترونى حيث جاء بنص المادة ٢٧٥ من قانون العقوبات المعدل بالمرسوم الصادر عام ٢٠٠١م الخاص بجرائم الحاسب الآلي بان يعاقب بالسجن لمدة لا تقل عن ثلاثة أشهر ولا تزيد على السنتين وبغرامة تتراوح بين مائة ريالً عماني إلى خمس مئة ريال أو بإحدى هاتين العقوبتين لكل من تعمد استخدام الحاسب الآلي في ارتكاب الأفعال الآتية :

أ ـ الالتقاط غير المشروع للمعلومات أو البيانات.

ب ـ الدخول غير المشروع على أنظمة الحاسب الآلي.

جـ ـ التجسس والتنصت على البيانات والمعلومات

د ـ انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم وتزوير البيانات أو الوثائق المبرمجة.

هـ ـ إتلاف وتغيير ومحو البيانات والمعلومات.

و ـ جمع البيانات والمعلومات وإعادة استخدامها.

ز ـ التعدي على برامج الحاسب الآلي سواء بالتعديل أو الاصطناع.

حـ ـ نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية.

وتنص المادة ٢٧٦ مكرر٣ على انه يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تتجاوز ألف ريال عماني على كل من :

أ ـ قام بتقليد أو تزوير بطاقة من بطاقات الائتمان أو السحب .

ب ـ استعمل أو حاول استعمال البطاقة المقلدة أو المزورة مع العلم بذلك .

جـ ـ قبل الدفع ببطاقة الائتمان المزورة أو المقلدة مع العلم بذلك

وتنص المادة ٢٧٦ مكرر ٤ على أنه يعاقب السجن لمدة لا تزيد على ثلاث سنوات وبغرامة لا تتجاوز خمسمائة ريال عماني على كل من :

أ ـ استخدم البطاقة كوسيلة للسحب مع علمه بعدم وجود رصيد لها .

ب ـ استعمل البطاقة بعد انتهاء صلاحيتها أو إلغائها وهو على علم بذلك .

جـ ـ استعمل بطاقة الغير بدون علمه[1] .

٤ ـ قطـر : أيضاً «وشأن سلطة عمان» تضمن التشريع العقابي القطري النص على عقوبات رادعة لمرتكبي جرائم الحاسب الآلي وكذا بطاقات الدفع الإلكتروني وذلك حيث جاء الفصل الخامس من الكتاب الثالث الباب الثالث من قانون العقوبات المعدل بالقانون رقم ١١ لسنة ٢٠٠٤ بعنوان جرائم الحاسب الآلي في المواد من ٣٧٠

(١) راجع النص الكامل للقانون على موقع وزارة العدل العمانية . . http:// www.moj.gov . .

الى٣٨٧ بتجريم العديد من الأفعال غير المشروعة المصاحبة لاستخدامات الحاسب الآلي وبطاقات الدفع الاليكتروني، حيث تنص المادة ٣٧٩ على أنه يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات، كل من استخدم حاسباً آليا بطريق التلاعب، سواء عن طريق إدخال معلومات، أو بيانات زائفة أو غير حقيقية، أو عن طريق العبث بالبرامج وهذه المادة يمكن أن تنطبق على كافة أفعال التصيد الاحتيالي لأرقام وبيانات بطاقات الدفع الإلكتروني.

وتنص المادة ٣٨٠ على أنه يعاقب بالحبس مدة لا تتجاوز ٥ سنوات، كل شخص ارتكب تزويراً في المستندات المعالجة آلياً، أياً كان شكلها، وترتب عليه الإضرار بالغير، أو استعمل هذه المستندات المزورة مع علمه بذلك.

ويعد تزويراً في برامج الحاسب الآلي أو البرامج المسجلة على ذاكرته للحصول على نتائج غير صحيحة.

وتنص المادة ٣٨١ على أنه يعاقب بالحبس مدة لا تتجاوز خمس سنوات كل من استولى، بغير حق، على أموال البنوك أو العملاء لديها عن طريق استخدام بطاقات الدفع الممغنطة التي يصدرها البنك، سواء أكانت خاصة به أو بعميل آخر.

وتنص المادة ٣٨٢ على «أنه يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تتجاوز ثلاث سنوات، وبالغرامة التي لا تقل عن عشرة آلاف ريال ولا تزيد على عشرين ألف ريال كل من:

أ- حاز أو استخدم آلات صنع بطاقات الدفع الآلي دون تصريح من الجهات المختصة.

ب ـ حاز أو أحرز بطاقة دفع آلي مزورة، أو مسروقة مع علمه بذلك.

جـ ـ حاز أو أحرز بطاقات دفع آلي معدة للإصدار دون تصريح بذلك من البنك.

د ـ حاز بغير تصريح من البنك آلات ومعدات طباعة بطاقات الدفع الآلي.

هـ ـ حاز أدوات مصرفية يدوية أو آلية مما يستخدم في إتمام التعامل ببطاقات الدفع الآلي دون تصريح بذلك».

وتنص المادة ٣٨٣ على « أنه يعاقب بالحبس مدة لا تقل عن سنة ولا تتجاوز خمس سنوات، وبالغرامة التي لا تقل عن عشرة آلاف ريال ولا تزيد على عشرين ألف ريال كل من :

أ ـ زور بطاقة دفع آلي.

ب ـ استعمل بطاقة دفع آلي مزورة، أو مسروقة مع علمه بذلك.

جـ ـ قبل بطاقات دفع آلي غير سارية، أو مزورة، أو مسروقة مع علمه بذلك.

د ـ صنع المعدات، أو الآلات المستخدمة في صناعة بطاقات الدفع الآلي بدون ترخيص».

وتنص المادة ٣٨٤ على : « أنه يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات وبالغرامة التي لا تزيد على عشرة آلاف ريال كل موظف بأحد البنوك أو المؤسسات المالية أو مكاتب الصرافة أو غير ذلك من الجهات الخاصة، بتلقي الأموال، أفشى أسرار المتعاملين معها، أو حصل عليها بدون مسوغ لإصدار بطاقات دفع آلي مزورة».

وتنص المادة ٣٨٦ على : «أنه في جميع الأحوال، يحكم برد المبالغ المستولى عليها وكذلك مصادرة كافة الآلات المصنوعة والمستخدمة في ارتكاب الجريمة المنصوص عليها في هذا الفصل»[١].

مادة ٣٨٧ : وتنص على أنه يعاقب على الشروع في الجنح المنصوص عليها في هذا الفصل، بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة التامة.

٥ ـ جمهورية مصر العربية : شأن قوانين العقوبات في غالبية الدول العربية، خلا قانون العقوبات المصري وتعديلاته المتتالية من أية نصوص تعاقب على الأفعال غير المشروعة المصاحبة لنشاط بطاقات الدفع الإلكتروني وقد لجأ القضاء المصري إلى تطبيق المواد التي تعاقب على جرائم السرقة والاحتيال والتزوير وخيانة الأمانة على هذا النوع من الجرائم وقد كان لصدور القانون رقم ١٥ لسنة ٢٠٠٤م بشأن تنظيم التوقيع الاليكتروني صدى واسع في حسم العديد من المشكلات القانونية التي كان يتصدى لها القضاء المصري بالاجتهاد، فجاء هذا القانون بتعريفات واضحة ومحددة لماهية المحرر الإلكتروني والوسيط الاليكتروني، كما تضمنت المادة ٢٣ من هذا القانون النص على : « مع عدم الإخلال بأية عقوبة أشد في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تتجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من :

(١) راجع النص الكامل للقانون على موقع شبكة المعلومات القانونية لدول مجلس التعاون الخليجي على عنوان http://www.gcc-legal.org

أ ـ أصدر شهادة تصديق اليكتروني دون الحصول على ترخيص بمزاولة النشاط .

ب ـ اتلف أو عيَّب توقيعاً أو وسيطاً أو محرراً اليكترونياُ، أو زوّر شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر .

جـ ـ استعمل توقيعاً، أو وسيطاَ أو محرراً اليكترونياً معيباً أو مزوراً مع علمه بذلك .

د ـ خالف أياً من أحكام المادتين ١٩ , ٢١ من هذا القانون(*) .

هـ ـ توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر اليكتروني أو اخترق هذا الوسيط أو اعترضه أو عطّله عن أداء وظيفته .

٦ ـ إمارة دبى : شأن باقي القوانين والتشريعات العقابية تطبق المواد المتعلقة بالسرقة والتزوير والاحتيال وخيانة الأمانة، ولا يوجد نصوص صريحة تجرم هذه الأفعال، إلا أن القانون رقم ٢ لسنة ٢٠٠٢م بشأن المعاملات والتجارة الإلكترونية قد نص في المادة ٣٢ من الفصل السابع على أنه مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر، يعاقب كل من ارتكب فعلاً يشكل جريمة بموجب التشريعات النافذة، باستخدام وسيلة اليكترونية بالحبس لمدة لا تزيد على ستة أشهر وبغرامة لا تتجاوز ١٠٠,٠٠٠

(*) تنص هاتان المادتان على ضوابط مزاولة نشاط إصدار شهادات التصديق الاليكتروني وحماية بيانات التوقيع الاليكتروني والوسائط الاليكترونية . راجع النص الكامل للقانون ولائحته التنفيذية، إصدارات الهيئة العامة لشئون المطابع الأميرية، القاهرة، ٢٠٠٥م .

درهم أو بإحدي هاتين العقوبتين، ويعاقب بالعقوبة الأشد إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذه المادة.

٧ـ المغرب : شأن معظم القوانين العقابية العربية، خلا أيضا القانون الجنائى المغربي من أية نصوص واضحة وصريحة تجرم هذه الأفعال، إلا أن الباب العاشر منه تضمن تعديلاً بتاريخ ١١ نوفمبر عام ٢٠٠٣م، بإضافة الفصول «المواد ٣/ ٦٠٧ حتى ١١/ ٦٠٧ «لتجريم كافة الأفعال غير المشروعة المتعلقة بنظم المعالجة الآلية للمعلومات وذلك على النحو التالي :

أ ـ الفصل ٣/ ٦٠٧ يعاقب بالحبس من شهر إلى ثلاثة أشهر وبالغرامة من ٢,٠٠٠ إلى ١٠,٠٠٠ درهم أو بإحدى هاتين العقوبتين فقط كل من دخل إلى مجموع أو بعض نظام للمعالجة الآلية للمعطيات عن طرق الاحتيال. ويعاقب بالعقوبة نفسها من بقي في نظام للمعالجة الآلية للمعطيات أو في جزء منه كان قد دخله عن طريق الخطأ وهو غير مخول له حق دخوله، وتضاعف العقوبة إذا نتج عن ذلك حذف أو تغيير المعطيات المدرجة في نظام للمعالجة الآلية للمعطيات أو اضطراب في سيره.

ب ـ الفصل ٤/ ٦٠٧ دون الإخلال بالمقتضيات الجنائية الأشد يعاقب بالحبس من ستة أشهر إلى سنتين وبالغرامة من ١٠,٠٠٠ إلى ١٠٠,٠٠٠ درهم كل من ارتكب الأفعال المشار إليها في الفصل السابق في حق مجموع أو بعض نظام للمعالجة الآلية للمعطيات أنه يتضمن معلومات تخص الأمن الداخلي أو الخارجي للدولة أو أسراراً تهم الاقتصاد الوطني.

دون الإخلال بالمقتضيات الجنائية الأشد ترفع العقوبة إلى الحبس من سنتين إلى خمس سنوات وبالغرامة من ١٠٠,٠٠٠ إلى ٢٠٠,٠٠٠ درهم إذا نتج عن الأفعال المعاقب عليها في الفقرة الأولى من هذا الفصل تغيير المعطيات المدرجة في نظام للمعالجة الآلية للمعطيات أو حذفها أو اضطراب في سير النظام أو إذا ارتكبت الأفعال من طرف موظف أو مستخدم أثناء مزاولة مهامه أو بسببها أو إذا سهل للغير القيام بها .

ج ـ الفصل ٦٠٧/٥ يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من ١٠,٠٠٠ إلى ٢٠٠,٠٠٠ درهم أو بإحدى هاتين العقوبتين كل من عرقل عمداً سير نظام للمعالجة الآلية للمعطيات أو أحدث فيه خللا .

د ـ الفصل ٦٠٧/٦ يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من ١٠,٠٠٠ إلى ٢٠٠,٠٠٠ درهم أو باحدي هاتين العقوبتين فقط كل من أدخل معطيات في نظام للمعالجة الآلية للمعطيات أو أتلفها أو حذفها منه أو غير المعطيات المدرجة فيه أو غير طريقة معالجتها أو طريقة إرسالها عن طريق الاحتيال .

هـ ـ الفصل ٦٠٧/٧ دون الإخلال بالمقتضات الجنائية الأشد، يعاقب بالحبس من سنة إلى خمس سنوات وبالغرامة من ١٠,٠٠٠ إلى ١,٠٠٠,٠٠٠ درهم كل من زور أو زيف وثائق المعلومات أيا كان شكلها إذا كان من شأن التزوير أو التزييف إلحاق ضرر بالغير .

دون الإخلال بالمقتضيات الجنائية الأشد تطبق العقوبة نفسها على كل من استعمل وثائق المعلومات المشار إليها في الفقرة السابقة وهو يعلم أنها مزورة أو مزيفة .

و ـ الفصل ٨/ ٦٠٧ يعاقب على محاولة ارتكاب الجنح المنصوص عليها في الفصول ٣ـ٦٠٧ إلى ٧ـ٦٠٧ أعلاه والفصل ١٠ ـ ٦٠٧ بعده بالعقوبة المطبقة على الجريمة التامة .

ز ـ الفصل ٩/ ٦٠٧ تطبق عقوبة نفس الجريمة المرتكبة أو العقوبة المطبقة على الجريمة الأشد على كل من اشترك في عصابة أو اتفاق تم لأجل الإعداد لواحدة أو أكثر من الجرائم المنصوص عليها في هذا الباب ، إذا تمثل الإعداد في فعل أو أكثر من الأفعال المادية .

حـ الفصل ١٠/ ٦٠٧ يعاقب بالحبس من سنتين إلى خمس سنوات وبالغرامة من ٥٠ ,٠٠٠ إلى ٢ ,٠٠٠ ,٠٠٠ درهم كل من صنع تجهيزات أو أدوات أو أعد برامج للمعلومات أو أية معطيات أعدت أو اعتمدت خصيصا لأجل ارتكاب الجرائم المعاقب عليها في هذا الباب أو تملكها أو حازها أو تخلى عنها للغير أو عرضها أو وضعها رهن إشارة الغير .

ط ـ الفصل ١١/ ٦٠٧ يجوز للمحكمة مع مراعاة حقوق الغير حسن النية أن تحكم بمصادرة الأدوات التي استعملت في ارتكاب الجرائم المنصوص عليها في هذا الباب والمتحصل عليه منها .

يمكن علاوة على ذلك الحكم على الفاعل بالحرمان من ممارسة واحد أو أكثر من الحقوق المنصوص عليها في الفصل ٤٠ من هذا القانون لمدة تتراوح بين سنتين وعشر سنوات .

يمكن أيضا الحكم بالحرمان من مزاولة جميع المهام والوظائف العمومية لمدة تتراوح بين سنتين وعشر سنوات وبنشر أو بتعليق الحكم الصادر بالإدانة[1].

٤ .٢ المواجهة الأمنية والجهود الدولية

برغم أن العديد من الدول العربية لديها أجهزة متخصصة في مكافحة هذا النوع من الجرائم، وأن تلك الأجهزة تبذل جهوداً فائقة في هذا المجال، إلا أن هناك دولاً أخرى مازالت تفتقر إلى هذا النوع من التخصص، حيث تعتمد أجهزة الشرطة عند فحص ما يرد إليها من بلاغات على الدعم الفنى الذي توفره لها أقسام الأخطار بالبنوك والمؤسسات المالية الكبرى.

وبرغم أهمية التعاون الدولي في هذا المجال حيث تعتمد ملاحقة مرتكبي هذا النوع من الجرائم على التنسيق المستمر وتبادل البيانات والمعلومات بين أجهزة المكافحة في الدول المختلفة إلا أن هذا التعاون مازال محدوداً للغاية، ليس على المستوى العربي فحسب، بل على المستوى الدولي أيضاً.

وتتطلب مواجهة هذا النوع من الجرائم ضرورة أن يتوافر لدى جهاز المكافحة المختص العديد من المقومات التدريبية والفنية والتقنية لكى ينهض بدوره.

ويعد الاهتمام بالعنصر البشري في عمليات المكافحة إحدى أهم مراحل المواجهة، حيث يلزم الأمر أن يكون الضباط والأفراد المعنيون

(١) راجع النص الكامل للمسطرة الجنائية على موقع وزارة العدل المغربية http:// www.justice.gov.ma.

بمكافحة هذا النوع من الجرائم على دراية تامة بآلية التعامل بها وأنواعها المختلفة وفوائدها وأخطارها والقوانين والأعراف المنظمة لها.

٤ .٢ .١ وحدة البحوث الفنية

في كثير من الحالات التي يتم كشفها والإبلاغ عنها من البنوك والمؤسسات المالية التي تنطوي على جرائم بطاقات الدفع الإليكترونى، فإن عمليات الفحص والمتابعة وإجراءات التحري والضبط قد تحتاج إلى معاونة فنية أكثر دقة، حتى يمكن تحقيق الربط بين البلاغات المماثلة، وإجراء عمليات التتبع الإلكتروني العكسي للحالات التي ترتكب من خلال شبكة الإنترنت، وهو الأمر الذى استلزم ضرورة إنشاء معمل لأعمال الفحص والمضاهاة وأعمال الحاسب الآلي الأخرى وذلك بالإدارة المختصة بمكافحة هذا النوع من الجرائم، وذلك بهدف تقديم المعاونة الفنية لضباط المكافحة ميدانياً[1].

ويحتوي هذا العمل على مجموعة من الأجهزة الفنية عالية التقنية التي تستخدم في عمليات الفحص والمضاهاة لكافة الوثائق والمستندات وبطاقات الدفع الإليكترونى وكذا أجهزة قراءة الأشرطة الممغنطة.

ومجموعة من الحواسب الآلية التي تحتوي ذاكرتها على أرشيف حصري لكافة الأصول المستخدمة في عمليات الفحص والمضاهاة.

ويباشر العمل في تلك الوحدة الفنية ضباط متخصصون في الكيمياء والهندسة الإلكترونية.

---

(١) تجدر الإشارة إلى أن إدارة مكافحة جرائم التزييف والتزوير بوزارة الداخلية بجمهورية مصر العربية تضم وحدة للبحوث الفنية متكاملة التجهيزات وتقوم بتقديم الدعم الفني لضباط المكافحة منذ عام ١٩٩٤م.

٤ .٢ .٢ التدريب المتخصص

يجب أن يتولى جهاز المكافحة المختص إعداد وتنظيم برامج تدريبية مكثفة وبشكل دوري لكل من :

١ ـ ضباط الشرطة : العاملين في الأوساط والمناطق ذات الطبيعة السياحية المعنيين بتلقي هذا النوع من البلاعات .

٢ ـ موظفي البنوك والمؤسسات المالية : وذلك لتوعيتهم والعمل على رفع كفاءتهم في كيفية التعامل مع هذا النوع من الجرائم وتقديم حالات الاشتباه والتصرف فيها .

٣ ـ التجار : خاصة في المراكز التجارية الكبرى لتدريبهم على كيفية الاشتباه في حالات الاحتيال والتحقق منها وربطهم هاتفياً مع مسئولي المكافحة .

ويعد التعاون والتنسيق بين جهاز المكافحة المختص بمواجهة هذا النوع من الجرائم ومراكز البطاقات بالبنوك والمؤسسات المالية أحد أهم عناصر المواجهة الأمنية ، بالإضافة إلى ضرورة الاهتمام بالمشاركة في الاجتماعات المحلية والإقليمية للمنظمات الدولية المعنية بهذا النوع من البطاقات مثل Master Card , Visa .

٤ .٢ .٣ الجهود الدولية لمواجهة جرائم بطاقات الدفع الإلكتروني

رأينا كيف أسهم التطور التكنولوجي في انتشار هذا النوع من الجرائم وكيف ألقت شبكة الانترنت بظلالها الكثيفة على هذه الأنشطة بعد أن أسهمت في تعزيز قدرات مرتكيبها وتمكينهم من الإيقاع بالمئات بل والآلاف من الضحايا في مختلف بقاع الأرض ، وكيف أصبح من المألوف

أن يكتشف حامل البطاقة في دولة ما أن بطاقته قد استخدمت في شراء سلعة من أحد المحلات « في دولة ثانية» ويكون الفاعل في دولة ثالثة وقد تمت الواقعة من خلال موقع المحل البائع على شبكة الانترنت .

لذا نستطيع أن نؤكد أن مكافحة هذا النوع من الجرائم لا يمكن أن تتحقق دون وجود نوع من التعاون الدولي والتنسيق المتبادل بين أجهزة المكافحة المختصة في هذا المجال .

وقد أفصح إعلان فيينا الصادر عن مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين عن القلق الذي يساور الدول الأعضاء في الأمم المتحدة إزاء الأثر الذي يخلفه ارتكاب الجرائم الخطيرة ذات الطبيعة الدولية على مجتمعاته، واقتناعها بضرورة التعاون الثنائي والإقليمي والعالمي في مجال منع الجريمة وتحقيق العدالة الجنائية، فضلا عن القلق « بشكل خاص» إزاء الجريمة المنظمة عبر الوطنية والارتباطات بين مختلف أشكالها وإدراك هذه الدول لضرورة تعزيز التنسيق والتعاون فيما بينها، بصدد مكافحة مشكلة الجريمة العالمية، باعتبار أن اتخاذ التدابير اللازمة في هذا الشأن، هو مسئولية عامة ومشتركة لهذه الدول[1] .

وحتى اليوم وبرغم مرور أكثر من خمسين عاماً على ظهور واستخدام بطاقات الدفع الإلكتروني على المستويين المحلي والدولي، فإننا لا نجد أية صيغة دولية لتنسيق التعاون الأمنى والقضائى في هذا المجال سوي من بعض الاتفاقيات والمعاهدات ذات الأطر العامة بشأن التعاون الأمني، أو القضائي سواء على المستوى الإقليمي، أو الدولي .

---

(١) مصطفى طاهر ، المواجهة التشريعية لظاهرة، غسل الأموال ، دار نهضة مصر، القاهرة ٢٠٠٢م، ص ٤٤٩ . . .

ويمكن أن نشير هنا إلى الدور المأمول لكل من معاهدة بودابست بشأن جرائم الحاسبات، المعلوماتية والاتصالات وكذا دور المنظمة الدولية للشرطة الجنائية في هذا الشأن

١ ـ معاهدة بودابست بشأن جرائم الحاسبات، المعلوماتية والاتصالات

بتاريخ ٢٣/ ١١/ ٢٠٠١م وفي مدينة بودابست عاصمة المجر، وقعت ٢٦ دولة أوروبية بالإضافة إلى كندا، اليابان، جنوب إفريقيا والولايات المتحدة الأمريكية أول معاهدة دولية بشأن الأفعال الإجرامية التي تتم من خلال نظم وشبكات الحاسب الآلي ونظم الاتصالات أو باستخدامها.

وتضم هذه المعاهدة ٤٨ مادة موزعة على أربعة فصول تتضمن تعريفات محددة لهذا النوع من الجرائم وسبل التعاون الأمني والقضائي وتتبع وتبادل المعلومات وتسليم الجناة وذلك على النحو التالي:

الفصل الأول: تعريفات خاصة ببعض المصطلحات الفنية «لتوحيد المفاهيم».

الفصل الثانى: ترتيبات لابد من اتخاذها على الصعيد المحلي:

القسم الأول: النصوص الجنائية الموضوعية

١ـ بشأن الجرائم ضد الخصوصية وسلامة وتواجد معلومات ونظم الحاسب الآلي..، ويشمل توصيفاً لأنواع متعددة من الجرائم.

٢ ـ بشأن الجرائم المتصلة بالحاسب الآلي، ويشمل استخدام الحاسب الآلي في التزوير وفي الأفعال الاحتيالية.

٣ـ الجرائم المتعلقة بالمحتوى والمضمون.

٤ ـ الجرائم المتصلة بالتعدي على حقوق المؤلف والحقوق المجاورة.

القسم الثاني : القانون الاجرائي : فيما يتعلق بالإجراءات الجنائية، ويشمل الحفاظ على المعلومات المخزنة والأوامر الخاصة بتسليم الأدلة وتفتيش وضبط بيانات الحاسب الآلي المخزنة وجمع البيانات في الوقت الفعلي و اعتراض المعلومات.

الفصل الثالث : مسائل التعاون الدولي وتسليم الجناة والمساندة المشتركة، الإجراءات، التعاون في التحريات و جمع بيانات المرور والحركة الخاصة بالبيانات وكذا إنشاء شبكة المنظومة الدولية [٢٤/ ٧] لكى تقوم كل دولة طرف بالاتفاقية بتخصيص نقطة اتصال متاحة طوال الأربع والعشرين ساعة يوميا وسبعة أيام أسبوعيا وذلك لضمان توافر تقديم المساعدات المباشرة لغرض التحقيقات أو الإجراءات الخاصة بالجرائم المتعلقة بنظم وبيانات الحاسب الآلي، أو لتجميع الأدلة الخاصة بالجريمة في شكل إلكتروني.

الفصل الرابع : ويتضمن مواد تتعلق بالانضمام والانسحاب من وتعديل المعاهدة وفض المنازعات والتشاور بين الأعضاء ورغم أن هذه المعاهدة هي في الأصل أوروبية المنشأة، إلا أنها دولية النزعة، وقد انضم إليها العديد من دول العالم [١].

---

(١) عمرو زكي عبد المتعال، المعاهدة الدولية لمقاومة جرائم الحاسبات، ورقة عمل مقدمة لمؤتمر الجوانب القانونية للتجارة القانونية للتجارة الإليكترونية- مقر جامعة الدول العربية- يناير ٢٠٠٢ م. وقدتم توزيع نص هذه المعاهد على الوفود التي شاركت فى المؤتمر الدولي الخامس للإجرام السيبيري الذي عقد في القاهرة خلال شهر أبريل ٢٠٠٥م، لحث الدول على الانضمام لها، ولم ينضم إليها حتى الآن أي من الدول العربية . ويمكن الاطلاع على النص الكامل للمعاهدة باللغات العربية والإنجليزية والفرنسية والأسبانية من خلال الموقع الخاص باتفاقيات الاتحاد الأوروبي . ,int†http://conventions.coe,

٢ ـ المنظمة الدولية للشرطة الجنائية « الانتربول» Interpol

الانتربول هو أكبر منظمة شرطية دولية في العالم، أنشئت عام ١٩٢٣م لتيسير التعاون الشرطي الجنائي عبر الحدود، ويضم اليوم ١٨٦ دولة عضوا، وهو يدعم ويساند جميع المنظمات والسلطات والأجهزة التي تضطلع بمهمة الوقاية من الإجرام الدولي ومكافحته.

وتيسر الأمانة العامة في ليون بفرنسا «حيث مقر المنظمة» منظومة اتصالات سريعة وموثقة للربط والاتصال بين أجهزة الشرطة في شتى أنحاء العالم، وتشمل نشاطاتها ذات الأولوية مجالات الأمن العام، الإرهاب، والإجرام المنظم، جرائم المخدرات، والإجرام المالي والمتعلق بالتكنولوجيا المتقدمة[١].

وفي عام ١٩٩٩م قامت المنظمة بتوقيع اتفاق تعاون مع عدد من المنظمات والمؤسسات المالية الدولية المسئولة عن إنتاج وتوزيع بطاقات الدفع الاليكتروني، بشأن التعاون في مواجهة جرائم بطاقات الدفع على المستوى الدولي.

وفي أغسطس من العام نفسه تم إعداد برنامج لتصنيف جرائم بطاقات الدفع على مستوى العالم من خلال موقع المنظمة على الشبكة الدولية ولا يسمح بالدخول لقاعدة البيانات المشار إليها سوى لمسئولي أجهزة المكافحة في الدول الأعضاء والمسئولين عن إنتاج وتوزيع تلك البطاقات من خلال كلمة مرور خاصة[٢]، Password ولارتباط هذا النشاط بجرائم تكنولوجيا

---

(١) راجع موقع المنظمة العام على شبكة الإنترنت http:// www.interpol.org . . .

(٢) يتم ذلك من خلال موقع المنظمة المؤمن على الشبكة https://www.interpol.int . وهو غير الموقع العام المتاح للكافة.

المعلومات، قامت المنظمة بتشكيل مجموعات عمل إقليمية أوروبية، أمريكية، آسيوية، إفريقية وكذا لجنة منسقة للعمل على تنسيق وتوجيه الجهود الدولية في مواجهة هذا النوع من الجرائم.

٣ ـ شبكة إتصال الانتربول (I-24/7)

تبنت المنظمة الدولية للشرطة الجنائية (الإنتربول) مهمة تنفيذ شبكة الاتصال «٢٤/ ٧» تفعيلاً لما ورد بالفصل الثالث من معاهدة بودابيست بشأن جرائم الحاسبات، المعلوماتية و الاتصالات، بهدف إتاحة الفرصة لأجهزة المكافحة من دول العالم المشتركة في هذه الشبكة لتبادل المعلومات الفنية وتتبع هذا النوع من الجرائم طوال الأربع والعشرين ساعة خلال أيام الأسبوع، إلا أن استجابة الدول النامية للاستفاده من هذه الوسيلة مازالت محدودة.

٤ ـ مشروع جولدفيش Gold Phish

بعد انتشار ظاهرة التصيد الاحتيالي عبر شبكة الانترنت تبنت منظمة الانتربول مشروع جولدفيش Gold Phish لتكثيف الجهود الدولية لمواجهة هذه الظاهرة منذ شهر يونيو ٢٠٠٥م بالمشاركة مع فرق عمل من عدة دول وصل عددها حتى الآن ٢٤ دولة « لم ينضم لهذا المشروع حتى الآن أي من الدول العربية » وذلك بهدف[١] :

١ ـ التنسيق في إجراء التحريات على المستوى الدولي لمواجهة هذا النشاط.

---

(١) كان للباحث شرف المشاركة مع فريق العمل الامريكي «من خلال المسئولين عن هذا المشروع بالمنظمة الدولية للانتربول» في فحص بلاغ شركة ويسترن يونيون الأمريكية، وتم تتبع وضبط العديد من مرتكبي هذه الجرائم داخل مصر خلال عام ٢٠٠٦م.

٢ ـ إعداد شبكة خاصة بفرق البحث المعينة في كل دولة .

٣ ـ اقتفاء أثر الأموال المسروقة ومتحصلات هذا النشاط في الدول المختلفة .

٤ ـ اتخاذ إجراءات وقائية لمنع هذه الجرائم على المستويين المحلي والدولي .

٥ ـ التحالف العالمي لمكافحة التصيد الاحتيالى على شبكة الانترنت

في ضوء التزايد الكبير لعمليات التصيد الاحتيالي عبر شبكة الانترنت Phising ، وتعرض الآلاف من مستخدميها في مختلف دول العالم للخسائر المادية نتيجة سرقة بيانات بطاقاتهم بهذا الأسلوب، ما أثر سلباً في حركة التجارة عبر مئات المواقع التجارية الشهيرة على الشبكة، الأمر الذى دفع المسئولين عن تلك المواقع إلى التكاتف لمواجهة هذا الخطر، فتم تشكيل تحالف عالمى لمواجهة هذه الظاهرة، انضم إليه ما يزيد على ١٦٠٠ من الشركات التجارية والمؤسسات المالية بما فيها المنظمات المسئولة عن بطاقات الدفع الاليكتروني مثل فيزا وماستركارد ومجموعة كبيرة من البنوك وشركات تكنولوجيا المعلومات[١]، وذلك بهدف استقطاب المعلومات الفنية حول المواقع والمصادر المتورطة في عمليات احتيال إلى قاعدة بيانات تدعى « شبكة تقارير الاحتيال «ما يتيح لجميع الأطراف المعنية، مثل مزودي خدمة الانترنت ISPs، أو المختصين في مجالات حماية المستهلك أو الشركات المتخصصة في الأمن المعلوماتي، إمكانية الاطلاع على أسماء تلك المواقع وإدراجها في مختلف البرمجيات وخدمات التصفح والبريد الإلكتروني

(١) راجع الموقع الرسمي لهذا التحالف على شبكة الإنترنت http:// www.antiphishing.org . . .

بحيث يتم التعرف عليها تلقائيا وحماية المستخدمين من أية عملية احتيال عبر الانترنت.

وكان من أهم نتائج نشاط هذه المجموعة أن قامت شركة مايكروسوفت Microsoft بطرح نسخة جديدة من برنامج التصفح الشهير الخاص بها على شبكة الانترنت «انترنت اكسبلورر٧» Internet Explorer7، بخاصية كشف المواقع[1] والرسائل الاحتيالية Anti- phishing حيث يمكن للمستخدم خلال قيامه بالتصفح عبر الشبكة التعرف على الرسائل والمواقع الاحتيالية بأن تظهر رسالة على شاشة الحاسب تحذره من ورود تقرير عن حالة احتيال بذات البيانات.

٦ ـ المؤتمرات الدولية

تشكل المؤتمرات الدولية فرصة كبيرة لتبادل الخبرات وتنسيق الجهود بين أجهزة المكافحة في هذا النوع من الجرائم من خلال أوراق العمل المقدمة من المشاركين التي تتضمن تجارب الدول، ودور الشركات المتخصصة في أمن الشبكات والمعلومات، من خلال ما يتم تطويره وتحديثه من نظم وبرامج متخصصة في مواجهة هذا النوع من الجرائم.

يتولى قسم مكافحة جرائم التكنولوجيا عالية التقنية بمنظمة الانتربول الإعداد لعقد مؤتمرات دورية مرة كل عامين في هذا المجال، كان آخرها المؤتمر الدولي الخامس للإجرام السيبيري الذي عقد في القاهرة خلال شهر أبريل ٢٠٠٥م.

---

(١) راجع موقع شركة مايكروسوفت http://www.microsoft.com. .

يتولى قسم الأخطار بمنظمتي الفيزا والماستر كارد العالمية إعداد وعقد مؤتمرات دورية سنوياً، يشارك فيها المختصون من أجهزة المكافحة في العديد من دول العالم، وكذا مسؤولو الأخطار بمراكز البطاقات بالمؤسسات المالية والمصرفية، بهدف الحد من تأثير هذا النوع من الجرائم على الأنشطة المالية والمصرفية.

تبنت شركة مايكروسوفت وهى من كبرى الشركات العاملة في نظم المعلومات إعداد وتنظيم مؤتمر يعقد سنوياً، يشارك فيه ممثلون عن الشركات المنتجة للبرمجيات وممثلو أجهزة المكافحة في دول العالم المختلفة بهدف إحداث نوع من التقارب والمواءمة بين ممثلي الشركات ومسئولي المكافحة والاطلاع على مستجدات هذه التكنولوجيا وتطبيقاتها المختلفة لمواجهة هذا الإجرام.

وهناك العديد من المؤتمرات الأخرى الإقليمية والدولية التي تتبناها بعض أجهزة المكافحة في دول العالم المتقدم وبعض البنوك والمؤسسات المالية الكبرى.

٤ .٣ الحلول الفنية في مواجهة جرائم بطاقات الدفع الإلكتروني

نظراً لتعدد أطراف كافة الحركات أو العمليات Transactions التي يتم إجراؤها بالبطاقات « مشروعة كانت أم غير مشروعة» وتنوع الجرائم المصاحبة لهذا النشاط، الأمر الذى يترتب عليه تعرض تلك الأطراف للخسائر وبشكل مستمر، لذا فإنه ليس من المتصور أن تقتصر إجراءات مواجهة هذا النوع من الجرائم على الجهات والأجهزة الحكومية فقط شرطية كانت أم قضائية، بل سعت المؤسسات المالية الدولية الراعية لهذه الأنشطة

مثل فيزا Visa ، ماستر كارد Master Card إلى طرح العديد من الحلول الفنية ووضع المعايير والأسس التي تحد وتفصل في النزاعات المتوقعة بين بنوك التجارة والبنوك المصدرة للبطاقات .

كما اتجهت البنوك إلى تطوير أنظمتها المصرفية وتأمين شبكات المعلومات الخاصة بها ، وتقديم كافة سبل الرعاية والدعم والمتابعة لحماية عملائها من التجار وحاملي البطاقات من الوقوع ضحايا هذا النوع من الجرائم .

٤ .٣ .١ الحلول الفنية في نطاق المؤسسات المالية والبنوك

قامت مؤسسة فيزا وماستر كارد بتطوير نظام S.E.T [١] ، لتأمين العمليات التي يتم إجراؤها على شبكة الإنترنت باستخدام بطاقات الدفع الإلكتروني . . ومن شأن هذا النظام تعريف التاجر بصاحب البطاقة حال التعامل بها عبر الشبكة والعكس ، مع تشفير البيانات التي يجري التعامل بها لحمايتها من أعمال القرصنة عبر الشبكة .

٤ .٣ .٢ التحول إلى البطاقات الذكية Smart Cards

وفي الإطار نفسه أيضا تسعى المؤسسات المالية الدولية المسئولة عن بطاقات الدفع الإلكتروني إلى حث وتحفيز البنوك في مختلف دول العالم إلى التحول من البطاقات الممغنطة إلى البطاقات الذكية ، حيث من المتوقع أن يؤدي انتشار هذا النوع من البطاقات إلى حدوث انخفاض كبير في حجم الجرائم التي يمكن أن ترتكب في هذا المجال ، إلا أن هناك العديد من العقبات

---

(١) هذه الأحرف اختصار لـ Sesure electronic transations . . . وتعني التحويلات الالكترونية المؤقتة .

التي تواجه البنوك، أهمها التكلفة العالية لإعادة تجهيز مراكز الإصدار، وإحلال وحدات البيع الاليكترونية POS المغنطة لدى التجار بأخرى تقبل التعامل مع نوعي البطاقات، وكذا الحال بالنسبة لماكينات الصرف الآلي.

وقد ابتكرت منظمة فيزا الدولية Visa بطاقة ذكية حديثة تحتوي على ذاكرة إلكترونية ومعالج صغير جداً Micro processor حيث يمكن لهذه البطاقة تخليق أرقام سرية مختلفة عقب كل عملية شراء يتم استخدام البطاقة فيها بمجرد الضغط بالإصبع على المعالج، وذلك لتأمين عمليات التعامل بالبطاقة سواء أكانت العمليات مباشرة مع التاجر أم من خلال الهاتف أو البريد الإليكترونى، وجاري طرحها قريباً.

٤ .٣ .٣ الحلول الفنية في نطاق البنوك

اتجهت العديد من البنوك خاصة في دول العالم المتقدم إلى تطبيق برنامج الشبكة العصبية Neoro net وهو أحد برامج الحاسب الآلي المستخدمة في مراكز الإصدار الذي يمكنه مراقبة كافة التعاملات التي تتم باستخدام البطاقات الخاصة بالبنك ذاته واكتشاف العمليات المشبوهة اليكترونيا في مهدها(*).

كما اتجهت بنوك أخرى إلى ضرورة الالتزام بان يكون عنوان شحن السلعة المشتراة عبر شبكة الانترنت هو ذاته عنوان صاحب البطاقة المدون لدى البنك.

(*) تم التعرف على تطبيقات هذا النظام بأحد البنوك الأمريكية الكبرى أثناء تلقينا لدورة تدريبية متخصصة في هذا النوع من الجرائم بالولايات المتحدة الأمريكية عام ١٩٩٩ وتبين حدوث انخفاض بنسبة ٥٠٪ من حجم الخسائر نتيجة تطبيق هذا النظام..

كما لجأت البنوك في العديد من دول العالم إلى منح عملائها بطاقات خاصة بالتعامل عبر شبكة الانترنت ذات حد ائتماني محدد ويمكن زيادته حسب طلب العميل للإقلال من حجم الخسائر التي يمكن أن يتعرض لها عملاؤها إذا ما تم سرقة بيانات تلك البطاقات من خلال مواقع الشبكة المختلفة.

كما طبقت بعض البنوك نظاماً يعتمد على استخدام خدمة الرسائل القصيرة SMS المستخدمة في الهواتف المحمولة «أو الجوالة» في إخطار عملائها بشكل فوري بكل عملية تستخدم فيها البطاقة، سواء أكانت سحب نقدي من ماكينات الصرف الآلي ATMs أو الشراء الطبيعي أو من خلال شبكة الانترنت، حتى إذا ما وصلت رسالة لصاحب البطاقة بشأن عملية لم يقم بإجرائها، فإنه سوف يقوم على الفور بمراجعة البنك الخاص به.

وهنا لا يفوتنا تأكيد ضرورة الاهتمام بموظفي مركز البطاقات بالبنك وبالأخص في نطاق بنوك التجار مع الاهتمام بتدريب الموظفين المسئولين عن الأخطار وكذا موظفي الموافقات على كيفية تحديد السلوك المالي المشبوه[1]، وأن يتم تدريبهم على طرح أسئلة معينة عند الرد هاتفياً على طلبات التجار بالحصول على موافقات أو متابعة الحركات الفورية الـ Monitoring وذلك لتحديد.

١ ـ أنواع التجار ذوي الأخطار العالية.

٢ ـ التجار الذين لديهم ماكينات إلكترونية ويتصلون بالبنك للحصول على موافقات على حركات تتم باستخدام الماكينات اليدوية.

---

(١) فهيم كامل فهيم، المرجع العملي لأعمال إدارة أخطار بطاقات الائتمان، البنك الأهلي المصري، ص ٤٢.

٣ـ الحركات ذات الأخطار العالية مثل حركة ذات مبلغ كبير تتم على بطاقة أجنبية .

ما يجب على التاجر اتباعه حتى لا يقع ضحية أحد أساليب الاحتيال بالبطاقات :

١ ـ يجب أن يكون التاجر ملماً بجميع عناصر الأمان بالبطاقة الائتمانية الصحيحة حتى إذا ما عرضت عليه بطاقة مزورة يستطيع كشفها .

٢ ـ في حالة إجراء الحركة الكترونيا يجب على التاجر مضاهاة البيانات المدونة على الإشعار المستخرج بالبيانات الموجودة على البطاقة المستخدمة فكثير من البطاقات المزورة يحوي شريطها الممغنط بيانات أخرى خلاف البيانات البارزة المدونة على البطاقة .

٣ـ التأكد من شخصية مقدم البطاقة وأنه بذاته صاحبها .

٤ ـ التأكد من أن توقيع صاحب البطاقة ذاتها لم يتعرض للمحو

٥ ـ التأكد من تطابق التوقيع المدون على البطاقة مع التوقيع الذى يوقعه مقدم البطاقة على إشعار الخصم .

٦ ـ عدم قبول أي بطاقة في التعامل تكون مقدمة من شخص آخر غير صاحبها .

٧ ـ يجب على التاجر الاحتفاظ بإشعارات الخصم أكبر فترة ممكنة ١٨ شهراً مع عدم تعريضها للإضاءه القوية في حالة الورق الحراري ـ حتى لا تتعرض بياناتها للمحو .

٨ ـ يجب على التاجر بما لديه من خبرة التعرف على العميل وملاحظته فإذا ما اشتبه فيه يقوم بالاتصال بالبنك .

٩ ـ أن يحرص التاجر على عدم تسوية المديونيات المالية بينه وبين تجار آخرين بالحصول منهم على إشعارات نفذت لدى هؤلاء التجار ويقدمها هو للتحصيل.

١٠ ـ متابعة العاملين لديه أثناء مباشرة البيع بموجب بطاقات الائتمان لأنه مسئول عن تجاوزاتهم.

١١ ـ عند طلب مقدم البطاقة تنفيذ عمليات بمبالغ كبيرة ومتعددة دون النظر لسعرها أو حاجته إليها يجب الاتصال بمركز البطاقات للاستفسار عن البطاقة وصاحبها.

ما يجب على صاحب البطاقة اتباعه حتى لا يقع ضحية لآخرين.

وهناك أخيرا العديد من المحاذير التي يجب على صاحب البطاقة التحوط لها وكذا النصائح التي يلزم عليه اتباعها وذلك على النحو التالي[1]:

١ ـ التوقيع على المكان المخصص لذلك خلف البطاقة بمجرد الحصول عليها.

٢ ـ حفظ الرقم الشخصي Pin في الذاكرة فور الحصول عليه، وعدم اطلاع أحد عليه، وفي حالة الاضطرار إلى كتابته في ورقة، عدم الاحتفاظ بها في ذات المكان الذي تحفظ فيه البطاقة.

٣ ـ وعند اختيار الرقم السري الابتعاد عن اختيار حروف وأرقام ذات صلة، حتى لا يصبح من السهل كشفها ومعرفتها كتاريخ الميلاد أو رقم الهاتف.

٤ ـ فحص فاتورة الشراء قبل التوقيع عليها.

---

(١) راجع كتيب «مجتمع اللا نقود»، من إصدارات منظمة الفيزا العالمية، ص ٢٥.

٥ ـ التأكد من استرداد البطاقة قبل مغادرة المكان الذي استخدمت فيه .

٦ ـ الاحتفاظ بنسخة من الفواتير أو الايصالات الدالة على استخدام البطاقة في عمليات الشراء، ومقارنتها بكشف الحساب الشهري للبطاقة .

٧ ـ عدم إعطاء رقم البطاقة لآخرين عن طريق الهاتف إلا في حالة التعامل مع شركة موثوق فيها وذات سمعة حسنة، أو في حالة المبادرة بإجراء المكالمة من جانب صاحب البطاقة .

٨ ـ إخطار البنك فور التأكد من عدم سلامة معاملة تضمنها كشف الحساب الوارد من البنك .

٩ ـ عدم ترك البطاقة تغيب عن البصر في كل مرة تستخدم فيها .

١٠ ـ عدم الاستجابة لرسائل البريد الإلكتروني «الخادعة» التي ترد منسوبة لبعض البنوك أو الجهات الأخرى، قبل التحقق من مصدرها .

١١ ـ عدم الإفصاح عن بيانات بطاقة الدفع الإليكترونى لدى مواقع غير آمنة على شبكة الإنترنت، وهناك العديد من الطرق التي يمكن التأكد من خلالها من تأمين الموقع .

١٢ ـ التأكد من إعدام الإشعارات والفواتير الخاصة بالشراء باستخدام البطاقات عند الرغبة في التخلص منها .

١٣ ـ الاهتمام بمراجعة كشوف الحساب الشهرية، وإخطار البنك بالعمليات غير الصحيحة فوراً .

١٤ ـ عدم التوقيع على إشعارات أو فواتير خالية من بيانات الشراء .

١٥ ـ في حالة مغادرة العنوان البريدي والانتقال إلى عنوان آخر ضرورة إخطار البنك بالعنوان الجديد في الوقت المناسب .

٤ .٣ .٤ الاستخدام الآمن لماكينات الصرف الآلي

ونظرا لتواجد ماكينات الصرف الآلي في الأماكن العامة فإنه يجب على حاملى البطاقات توخي الحذر أثناء استخدام هذه الماكينات، واتباع النصائح التالية :

١ ـ توخي الحذر من البيئة المحيطة، والابتعاد في حالة الارتياب في أحد الأشخاص بالقرب من الماكينة .

٢ ـ التوجه إلى ماكينة الصرف الآلي بصحبة أحد المعارف في حالة الاضطرار إلى استخدام الماكينة ليلاً .

٣ ـ من اللائق الانتظار بعيدا عن الماكينة حتى ينتهي الآخرون من استخدامها .

٤ ـ مراعاة الحذر أثناء إدخال الرقم السري Pin بحيث لا يتمكن أحد من رؤيته .

٥ ـ الحفاظ على سرية الحساب وعدم الإهمال في الحفاظ على الإيصال الصادر من الماكينة أو إلقائه بجوارها .

٦ ـ التأكد من استرداد البطاقة قبل الابتعاد عن الماكينة .

٧ ـ في حالة حدوث أي عطل بالماكينة مع عدم التمكن من استرداد البطاقة، يجب إخطار البنك فوراً .

الفصل الخامس

نماذج تطبيقية لجرائم بطاقات الدفع الإلكتروني

٥ . نماذج تطبيقية لجرائم بطاقات الدفع الإلكتروني

تعرضنا في الفصول السابقة للأنماط الاحتيالية المختلفة لجرائم بطاقات الدفع الإلكتروني، كما أوضحنا انعكاسات التطور التكنولوجي على هذا النوع من الجرائم وخاصة فيما يتعلق بعمليات اختلاس وسرقة بيانات بطاقات الدفع الإلكتروني.

ولمزيد من الإيضاح، وحتى تكتمل الصورة فإننا نستعرض في هذا الفصل العديد من نماذج البلاغات والوقائع التي تم فحصها، وكذا ما تم ضبطه من قضايا وكيفية معالجتها أمنياً، وذلك في ثلاثة مباحث، فنعرض في المبحث الأول نماذج من الجرائم الفردية وتواطؤ التجار، بينما نعرض في المبحث الثاني بعض قضايا جرائم البطاقات المرتبطة بتكنولوجيا المعلومات، وأخيراً المبحث الثالث فإننا نورد بعض نماذج لقضايا تورط فيها موظنو مراكز البطاقات لدى بعض البنوك، لتأكيد أهمية وجود نظم صارمة للرقابة الداخلية في تلك المراكز[1].

٥ .١ الجرائم الفردية وتواطؤ التجار

نتعرف في هذا المبحث على بعض النماذج التطبيقية لجرائم بطاقات الدفع الإليكترونى وتشمل:

- استصدار بطاقات صحيحة بموجب مستندات مزورة.
- استعمال البطاقات المسروقة والمفقودة.

---

(١) جميع الجرائم التى تم كشفها والقضايا التى تم ضبطها، الواردة في هذا الفصل من واقع أرشيف الإدارة العامة لمباحث الأموال العامة بوزارة الداخلية.

ـ تزوير الإشعارات والفواتير وتواطؤ التجار.

ـ مغافلة التجار.

٥ .١ .١في مجال استصدار البطاقات بموجب مستندات مزورة

تبلغ من مسئولي البطاقات بأحد البنوك باكتشاف قيام بعض الأشخاص بالتقدم للبنك لاستصدار بطاقات ائتمان صحيحة بموجب مستندات مزورة، واستخدام تلك البطاقات في عمليات الشراء وصرف مبالغ مالية عن طريق ماكينات الصرف الآلي المنتشرة داخل البلاد، دون سداد قيمة تلك المديونيات للبنوك، استناداً إلى عدم تمكن البنك من التوصل إليهم.

اتضح من الفحص أن بعض الأشخاص قد تمكنوا من خداع موظفي بعض البنوك وتقدموا بمستندات عبارة عن بطاقات إثبات شخصية وبعض السجلات التجارية المزورة وبعض الخطابات المنسوبة لشركات قطاع خاص وهمية لإثبات قيمة الدخل السنوي مدعومة بشهادات بنكية مصطنعة منسوبة للعديد من البنوك المختلفة تفيد خلافا للحقيقة أن طالب البطاقة له ودائع بالبنوك بمبالغ كبيرة «حتى يمكن زيادة الرصيد الائتماني للبطاقة».

تم وضع خطة بحث استهدفت تحديد نطاق استخدام تلك البطاقات والبنوك الصادرة منها وأشخاص مستخدميها، حيث اتضح من الفحص الذى تم إجراؤه على الحالات المكتشفة من البنك في إطار خطة البحث المشار إليها أن وراء هذا النشاط تشكيلاً عصابياً مكوناً من أربعة أفراد يضم عاطلاً ومندوب مشتريات وفني طباعة ومحاسب.

وبعد تقنين الإجراءات تم إعداد عدة أكمنة ثابتة ومتحركة ومتزامنة في أماكن متفرقة، التي تحددت لتسليم أحد المتهمين بطاقة ائتمانية مرسلة له

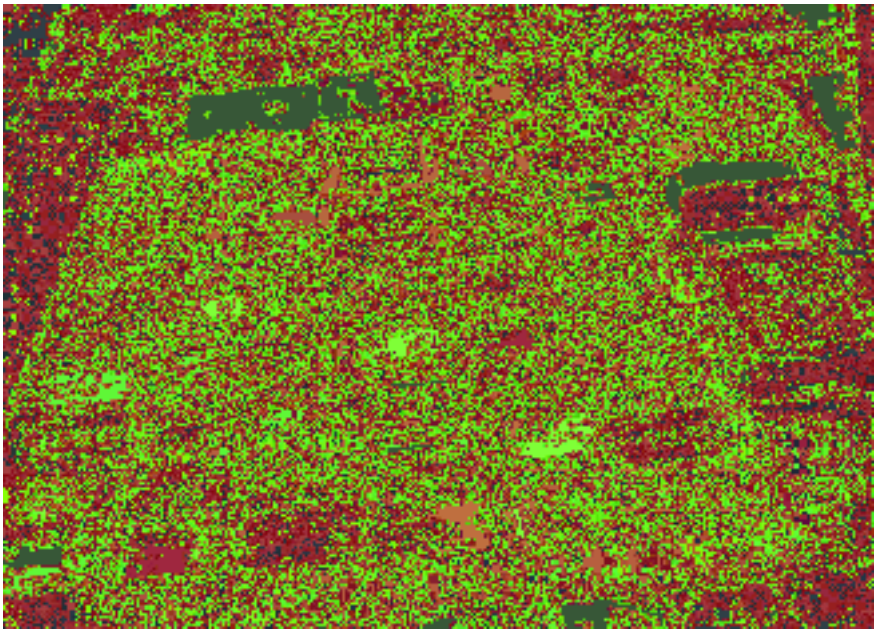
من احد البنوك بواسطة مندوب شركة بريد خاصة، حيث أمكن ضبط المذكور واستكملت إجراءات البحث التي أسفرت عن ضبط باقي أفراد التشكيل وضبط بحوزتهم ما يلي :

١ ـ عدد سبع وثلاثين بطاقة ائتمانية صادرة من بنوك مختلفة جميعها سارية بأسماء منتحلة وصور مختلفة لأفراد التشكيل .

٢ ـ كمية كبيرة من السجلات التجارية بأسماء مختلفة لأفراد التشكيل مصحوبة بكشوف حساب وشهادات بنكية مزورة منسوبة للعديد من البنوك .

٣ ـ كمية كبيرة من صور بطاقات إثبات الشخصية المزورة التي تحمل أسماء منتحلة وصوراً لأفراد التشكيل .

٤ ـ كمية كبيرة من إشعارات الخصم التي تفيد قيام أفراد التشكيل باستخدام البطاقات المضبوطة بمبالغ مالية كبيرة .



وبمواجهة أفراد التشكيل اعترف كل منهم بنشاطه وتحرر بشأن الواقعة المحضر اللازم وتم عرض المتهمين والمضبوطات على النيابة العامة.

٥ .١ .٢ استعمال البطاقات المسروقة والمفقودة

وفي هذا الإطار تبلغ للإدارة بالقاهرة من أحد البنوك العربية بأن المدعو م. ع. ج. قد غادر دولته إلى القاهرة باسم منتحل يدعى ف. ع. س وانه يستخدم بطاقة ائتمان ماستر كارد مبلغ بسرقتها، وبلغت قيمة تعاملاته بها حوالي ثمانين ألف دولار أمريكي، وأن مركز البطاقات بالبنك قد تأكد من صحة تلك المعلومات بعد أن تم حصر العمليات التي استخدمت بها تلك البطاقات في القاهرة.

أسفرت التحريات التي أجريت حول المذكور بالقاهرة ـ بعد مراجعة مراكز البطاقات ببعض البنوك المصرية ـ عن تحديد الأماكن التي يتردد عليها، فتم ضبطه حال تردده على أحد الملاهي الليلية وعثر بحوزته على جواز سفر بصورته بالاسم المنتحل وكمية من بطاقات الائتمان بعضها مبلغ بسرقته والبعض الآخر بالاسم المنتحل وقد أمكن الاستدلال على أصحاب بعض المحال التجارية التي تردد عليها المذكور مستخدماً البطاقات المسروقة، حيث تعرفوا عليه، وبمواجهته اعترف بنشاطه، وبعرضه على النيابة العامة أمرت بحبسه على ذمة التحقيق.

٥ .١ .٣ في مجال تزوير الإشعارات والفواتير وتواطؤ التجار

سبق أن أوضحنا أن بطاقات الدفع الاليكتروني تشكل أحد أهم بدائل النقود التي تسمح لحاملها باستخدامها في تمويل مشتريات وما يحصل عليه من خدمات دون التقيد بحدود الدولة التي يقيم بها، لذا كانت أهميتها لدى السائحين في كافة بلدان العالم.

وفي هذا الإطار كان قد تبلغ من وزارة السياحة بجمهورية مصر العربية بتضرر بعض السائحين الفرنسيين من تعرضهم للاحتيال من خلال استخدام بطاقاتهم الائتمانية في عمليات شراء وهمية بعد مغادرتهم البلاد، وهو ما حدا ببعض شركات السياحة الفرنسية إلى توجيه النصح لعملائها بتوخي الحذر عند استخدام بطاقاتهم الائتمانية داخل مصر، الأمر الذي يسئ إلى سمعة البلاد، وينذر بإهدار الجهود التي تبذلها الدولة لدفع وتشجيع التدفق السياحي إلى مصر.

تم وضع خطة بحث شاملة استهدفت تحديد وضبط القائمين بهذا النشاط الإجرامي، كان أهم بنودها :

١ ـ تحديد الشركات السياحية التي تضرر عملاؤها من هذا الأسلوب وكذا الفنادق والأماكن السياحية التي ترددوا عليها، وأرقام البطاقات الائتمانية لهؤلاء السائحين.

٢ ـ تحديد مواعيد وصول ومغادرة تلك الأفواج السياحية للبلاد.

٣ ـ مراجعة مراكز البطاقات بالبنوك التي تتعامل بهذا النظام، وتحديد عمليات البيع المرتدة خلال الفترة السابقة وبيانات البطاقات الائتمانية التي استخدمت فيها، وكذا المحال والمنشآت السياحية التي تمت بها والمبالغ التي صرفت مقابلها.

٤ ـ تجنيد المصادر السرية وتوسيع دائرة الاشتباه بالأوساط التجارية والمنشآت السياحية المتعاملة بهذا النظام، للحصول على أكبر قدر ممكن من المعلومات الداعمة لجهود البحث.

وتنفيذاً لهذه الخطة أمكن تحديد تشكيل عصابي وراء هذا النشاط يضم ثلاثة عشر متهماً من أصحاب المنشآت السياحية والعاملين بها بكل من

القاهرة، الأقصر، الغردقة، الذين تخصصوا في الاحتيال على أعداد كبيرة من السائحين والاستيلاء على مبالغ مالية كبيرة من حسابات بطاقاتهم الائتمانية وبعد تقنين الإجراءات تم ضبط جميع أفراد التشكيل وبحوزتهم مايلى :

أ ـ عدد ثمان ماكينات يدوية خاصة بثلاثة بنوك مصرية بعضها حيازة مشروعة والآخر يتم تداوله بصورة غير مشروعة بين أفراد التشكيل .

ب ـ كمية كبيرة من الإشعارات المزورة الخاصة بعمليات البيع الوهمية .

جـ ـ كمية كبيرة من الإشعارات التي تحمل بصمات بطاقات ائتمانية خاصة بأجانب بعضها ممهورة بتوقيعات مزورة لأصحاب تلك البطاقات، وكان من المزمع صرف قيمتها من بعض البنوك والشركات .

أفراد التشكيل العصابي وجانب من المضبوطات

وقد اتضح قيام بعض أفراد التشكيل« سائقي حافلات سياحية » بالعبث بمتعلقات السائحين الفرنسيين حال تركها بالأتوبيسات السياحية والحصول على بصمات بطاقاتهم الائتمانية، على إشعارات الخصم باستخدام ماكينات بطاقات الدفع اليدوية التي ضبطت بحوزتهم. تم بيع تلك الإشعارات أو تبادلها لإجراء عمليات شراء وهمية عليها من خلال المحلات والمعارض المملوكة لباقي أفراد التشكيل وتم تحصيل قيمة تلك الإشعارات من البنوك خصما من حسابات السائحين الأجانب «الضحايا» الذين لا يتسنى لهم اكتشاف هذه الخصومات إلا بعد مراجعة كشوف حساباتهم البنكية لدى عودتهم إلى بلادهم.

قدر إجمالي المبالغ التي استولى عليها أفراد التشكيل بحوالي المليوني جنيه.

٥ .١ .٤ كشف الثغرات الأمنية وعلاجها

كشفت عمليات الفحص والمتابعة أثناء إجراءات ضبط أفراد التشكيل العصابي المشار إليه عن وجود العديد من الثغرات في النظم المتبعة داخل مراكز البطاقات بالبنوك، التي استغلها أفراد التشكيل في نشاطهم الآثم، تمثلت فيما يلي :

١ ـ عدم قيام مراكز البنوك بإجراء استعلام ميداني جاد عن التجار وأصحاب المنشآت السياحية من راغبي التعامل بنظام البطاقات، أو الكشف عنهم جنائيا قبل إتمام إجراءات التعاقد، وانعدام وجود متابعة ميدانية لاحقة لنشاط هؤلاء التجار وأصحاب المنشآت، حيث لوحظ أن أحد المتهمين قد تعاقد مع أحد مراكز الإصدار بصفته صاحب معرض تأجير سيارات بناحية المعادي بالقاهرة

وحصل على ثلاث ماكينات يدوية» تحت زعم أنها للمعرض وفرعية بالقاهرة وشرم الشيخ وقام بإرسالها جميعا إلى بعض أفراد التشكيل بمدينة الغردقة وتم استخدامها في ارتكاب بعض الوقائع محل البلاغ، كما أن بعض أفراد التشكيل من التجار قد تم التعاقد معهم رغم كونهم محكوماً عليهم في قضايا مختلفة.

٢ـ عدم وجود جهة مركزية تتجمع لديها المعلومات بشأن التجار الذين ارتكبوا جرائم مماثلة سابقة أو سهلوا للغير ارتكاب مثل هذه الجرائم، في ظل عدم وجود تنسيق بين مراكز البطاقات بالبنوك المصرح لها بالتعاقد مع التجار وأصحاب المنشآت السياحية للتعامل بالبطاقات، حيث لوحظ أن بعض المتهمين الذين تم ضبطهم في تلك الواقعة مارسوا نشاطهم باستغلال تعاقدهم مع بنك(ع. أ. د) رغم سابقة قيام البنك. بإلغاء التعاقد معهم لإساءتهم استخدام الماكينات المسلَّمة إليهم و لورود العديد من عمليات البيع المرتدة إليهم من الخارج.

٣ـ افتقار مراكز إصدار البطاقات بالبنوك إلى أي نظم تحليل لبيانات إشعارات نشاط التاجر أو صاحب المنشأة وحجم عملياته المقدمة للبنك، والربط بينها وبين الاعتراضات المرتدة من الخارج، واستخلاص الأنشطة المشبوهة، والتصرف مع التجار وأصحاب المنشآت السياحية بموجب ما يتم التوصل إليه من نتائج حسبما هو متبع مصرفيا في العديد من الدول.

٤ـ أدلى بعض المتهمين باعترافات تفصيلية تؤكد استيلاءهم على مبالغ مالية تجاوزت المليوني جنيه من البنوك نتيجة الثغرات المشار إليها. . ولدى قيام الإدارة بمراجعة مراكز البطاقات بتلك البنوك أفاد

مسئولوها باستيلاء هؤلاء المتهمين على مبالغ تقل عن ذلك بكثير «ولا تزيد على نصف المليون»حيث اتضح من الفحص والمتابعة أن التجار وأصحاب المنشآت السياحية يحصلون على قيمة تلك العمليات، باعتبارها عمليات مشروعة استناداً إلى أن مراكز الإصدار بالبنوك تقوم ببعض عمليات المماطلة مع البنوك الأجنبية ببنوك السائحين لدى مراجعة العمليات المرتدة، استناداً إلى إصرار التجار على أنها عمليات مشروعة.

٥ ـ برغم أن ماكينات البيع الإلكترونية أكثر تأميناً وضماناً من ماكينات البيع اليدوية، إلا أنه لوحظ أن مراكز الإصدار بالبنوك المختلفة تستجيب لرغبات غالبية التجار في التعامل بماكينات البيع اليدوية فقط التي يجب أن يتم صرفها في أضيق الحدود.

٦ ـ برغم أن إشعارات البيع اليدوية المنسوبة لمراكز الإصدار بالبنوك المختلفة تحمل أرقاماً مسلسلة، إلا أنه لوحظ عدم وجود التزام متبادل بين تلك المراكز والمتعاقدين معها من التجار وأصحاب المنشآت السياحية في مصر لتنفيذ عمليات البيع على الإشعارات وفقاً لأرقامها المسلسلة المسلمة لذات التاجر وعدم قبولها أو صرف قيمتها لتاجر آخر.

٧ ـ كشفت المتابعة أيضاً عن وجود قصور معرفي بآلية التعامل بالبطاقات لدى العديد من أجهزة الشرطة الأخرى المعنية بتلقي مثل هذا النوع من البلاغات وعدم توافر الدراية الفنية المطلوبة لفحصها وكيفية إقامة الدليل ضد مرتكبيها قبل ضبطهم، الأمر الذي يؤثر سلباً في مستوى وفاعلية الأداء بهذه الأجهزة.

٨ـ اعتمد أفراد التشكيل على خطأ شائع في مجال البطاقات وهو اعتياد حاملي البطاقات على عدم مراجعة كشوف الحساب الخاصة بهم خاصة من الأجانب الذين يعتمدون في حياتهم اليومية على استخدام البطاقات .

٩ـ وتم إخطار البنك المركزي وكافة البنوك العاملة في هذا المجال لتلافي وسد تلك الثغرات .

٥ . ١ . ٥ مغافلة التجار

وفي هذا الإطار تبلغ من مسئولى مركز بطاقات بنك مصر باكتشافهم قيام بعض المحال التجارية «رضوان العجيل ـ راية ـ صادكو ـ اثير ـ شنكو» بإتمام عمليات بيع باستخدام بطاقة منسوبة لبنك ABC دون الحصول على موافقات صحيحة من البنك حال تنفيذه هذه العمليات . . وتمكن مستخدمها من الاستيلاء على قيمة تلك العمليات التي بلغت خمسين ألف جنيه .

أسفر الفحص الفني لتلك العمليات عن إتمامها بالتحايل على الماكينات الإلكترونية المتواجدة بتلك المحال بفصلها عن الاتصال بالبنك وإدخال أرقام موافقات وهمية عليها ، وترتب على ذلك قيام الماكينة بإخراج إشعارات خصم تبدو وكأنها صحيحة ، انخدع فيها أصحاب المحال .

أسفر فحص تحريات إدارة مكافحة جرائم التزييف والتزوير عن أن وراء ارتكاب تلك الوقائع المدعو «أ . ن . ع . » مدير محل بيع هواتف محمولة ومقيم إمبابة ـ جيزة . . إذ استغل المذكور خبرته في التعامل بنظام بطاقات الدفع وقيامه بمغافلة أصحاب تلك المحال التجارية أثناء إتمام العمليات بالأسلوب المشار إليه ، وتمكن من الاستيلاء على ثلاثين جهاز تليفون محمول .

تم التنسيق مع بنك مصر وإعداد نشرة بأوصاف المذكور وبيانات بطاقاته الائتمانية التي بحوزته ونشرها على محلات بيع أجهزة التليفونات المحمولة حيث أسفر ذلك عن ضبطه حال تردده على أحد تلك المحال بشارع مصدق بالدقى وشروعه في الاحتيال على مسئولى ذلك المحل بذات الأسلوب، وعثر بحوزته على سبع بطاقات ائتمانية منتهية الأرصدة باسمه منسوبة لبنوك(ABC ـ سيتى بنك ـ مصر ـ الأهلى ـ باركليز) التي استخدمها في ارتكاب الوقائع محل البلاغ وكذا مبلغ تسعة عشر ألف جنيه من متحصلات نشاطه.

بمواجهته أقر بارتكابه للوقائع وأرشد عن عدد (١٢) جهازاً من إجمالي الأجهزة المستولى عليها وعن الإرشاد عن باقي الأجهزة لبيعها لأشخاص لا يعلمهم وأبدى استعداده لسداد قيمتها وأخطرت النيابة العامة التي باشرت التحقيق.

٥ . ١ . ٦ في مجال استعمال البطاقات المزورة (تزوير كلي)

تبلغ من مركز البطاقات بأحد البنوك الكبرى، باشتباه أحد محال المجوهرات بمركز تجاري بمدينة نصر في سلامة بطاقة ائتمانية استخدمها أحد الأشخاص جورجي الجنسية في شراء مشغولات ذهبية بمبلغ خمسة آلاف جنيه اتضح بالانتقال والفحص تورط كل من :

ـ المدعو .D.M جورجي الجنسية ومقيم بالجيزة.

ـ المدعو G.M.B جورجي الجنسية ومقيم بالجيزة.

حيث وصل المذكوران للبلاد لغرض السياحة وقاما باستخدام عدة بطاقات ائتمانية مزورة في شراء كمية من المشغولات الذهبية والسلع الثمينة من بعض المحال التجارية بمناطق الدقي والمهندسين ومدينة نصر.

تم ضبط الأول حال شروعه في إتمام عملية الشراء محل البلاغ وبحوزته ثلاث بطاقات ائتمانية مزورة تزويراً كليًا وخمسة إشعارات خصم تفيد استخدامه للبطاقات المشار إليها في عمليات شراء رسمية، وكذا مشغولات ذهبية وزن مائة وخمسة وأربعين جراماً وجهاز هاتف محمول تبين شراؤه بتلك البطاقات.

بتطوير مناقشة المتهم الأول، أمكن تحديد مكان اختباء المتهم الثاني بإحدى الشقق المفروشة بمنطقة المهندسين حيث تم ضبطه وبحوزته كمية من الملابس والسلع الثمينة وقيمة مشترياتهم بذات البطاقات.

وبمواجهة المتهمين اعترفا بنشاطهما وأنهما تحصلا على تلك البطاقات عن طريق سيدة من جورجيا أمكن تحديدها وإخطار الإنتربول بشأنها.

تحرر بشأن تلك الواقعة المحضر اللازم وتم عرض المتهمين والمضبوطات على النيابة العامة.

٢.٥ نماذج تطبيقية لجرائم البطاقات المرتبطة بتكنولوجيا المعلومات

سبق أن أوضحنا في متن دراستنا كيف أثرت ثورة تكنولوجيا المعلومات في هذا النوع من الجرائم، وكيف تهيأت الفرصة لمرتكبيها لاصطياد ضحاياهم من دول أخرى، حتى إن بعض الشبكات الإجرامية قد اتخذت شكل الجريمة المنظمة عبر الوطنية، من حيث تعدد أعضائها، وتوافقهم الفكري، وكيفية تجميع وتوزيع عائدات أنشطتهم غير المشروعة وتواجدهم في عدة دول، ولا تجمع بينهم سوى بعض المواقع على شبكة الإنترنت.

ونعرض فيما يلي لبعض نماذج من هذا النوع من الجرائم :

القضية الأولى: تزوير البطاقات «جزئياً» بتلقين الشريط الممغنط لبيانات مختلفة:

تبلغ من مسئولي أحد محال تجارة الأجهزة الإلكترونية بالقاهرة بالاشتباه في سلامة بيانات بطاقة دفع اليكترونية، تقدم بها أحد الأشخاص للمحل لشراء هاتفي محمول. . بالانتقال الفوري للمحل المشار إليه، تبين وجود أحد الأشخاص يدعى أ. أ. م. مواليد ١٩٨٣م طالب بالجامعة ومقيم بالإسكندرية وبحوزته بطاقتا دفع إليكتروني تحملان بياناته، شارعاً في شراء هاتفين محمولين قيمتهما ٧٠٠٠ سبعة آلاف جنيه، وقد ارتاب موظف المحل في أمره لسابقة تردده على المحل منذ أسبوعين وشرائه جهازي تليفون محمول من ذات الماركة بموجب بطاقة أخرى، «كان قد أفاد البنك بعد انصرافه أأن العملية مرفوضة»، ولدى اصطحاب المذكور والبطاقتين للإدارة تبين أن برفقته آخرين هما كل من م. ى. أ مواليد ١٩٨٢م، م. م. ف. مواليد ١٩٨٤ وهما طالبان في الجامعة ويقيمان بالإسكندرية.

وبفحص البطاقتين المضبوطتين فنياً، تبين أنهما مزورتان عن طرق تلقين الشريط الممغنط ببيانات بطاقتين لأجانب آخرين، وبمواجهة المتهم المذكور اعترف باستعماله للبطاقات المزورة التي يتم إعدادها وتزويرها بمعرفة مرافقه م. ى. أ وبمواجهة الأخير اعترف بقيامه بتزوير البطاقات باستخدام وحدة تكوين البيانات الممغنطة الكترونياً وجهاز حاسب آلي بمسكنه بمدينة الإسكندرية.

بعد تقنين الإجراءات تم استهداف مساكن المتهمين الثلاثة حيث عثر بمسكن المتهم الأول الأخير م. ى. أ على ما يلي:

١ ـ جهازي حاسب آلي وبعض الإسطوانات المدمجة. CDs

٢ ـ جهاز قراءة وتكويد البيانات الخاصة بالبطاقات الممغنطة.

٣ـ عشرين بطاقة بلاستيك ممغنطة خام معدة للتزوير .

٤ـ ست بطاقات ائتمانية بأنواع مختلفة بعضها باسم المتهمين والبعض الآخر بأسماء أجنبية .

٥ـ خمسة وثلاثين إشعار خصم اليكتروني لمشتريات تم إجراؤها قيمتها ٩٨,٧٩٩ ألف جنيهاً باستخدام بطاقات مزورة .

٦ـ صور ضوئية لبطاقات دفع إليكتروني منسوبة لبعض البنوك الأجنبية .

٧ـ وبفحص جهازي الحاسب الآلي والأسطوانة تبين تحميلهم لملفات تحوى :

أ ـ أعداداً كبيرة الأرقام لبطاقات ائتمان منسوبة لبنوك في دول مختلفة ، تطابقت أعداد منها مع ذات الأرقام المبينة بإشعارات الخصم والبطاقات المضبوطة بحوزة المتهمين .

ب ـ صوراً لوجهي بطاقات ما ستر كارد وأميركان اكسبريس موضحاً عليها عناصر البطاقات ووسائل تأمينها .

جانب من المضبوطات «بطاقات، وحدة التكويد، وجهاز الحاسب»

بتطوير مناقشة المتهمين قرر المتهم الأخير بتحصله على أرقام البطاقات من أحد الأجانب من محترفي هذا النشاط من خلال أحد مواقع الدردشة على شبكة الإنترنت وقام بشراء وحدة قراءة وتكويد البطاقات الممغنطة من أحد المواقع التجارية على الشبكة المشار إليها، التي وصلته عن طريق البريد DHL بعد أن حول قيمتها بواسطة شركة ويسترن يونيون . وتحرر بشأن الواقعة المحضر اللازم وتم عرض المتهمين والمضبوطات على النيابة العامة للتصرف

القضية الثانية: اشتباه في عمليات شراء

تبلغ من أحد البنوك الوطنية الكبرى باشتباه مركز البطاقات في سلامة عدة عمليات شراء تمت بأحد محال المفروشات بأحد المراكز التجارية الكبرى بالقاهرة بلغ إجمالها سبعة آلاف وستمائة جنيه اتضح من الفحص السريع واللاحق بالتنسيق مع مركز البطاقات بالبنك أن تلك العمليات قد تمت باستخدام بطاقة ائتمانية منسوبة لمؤسسة ميريل لينش بالولايات المتحدة الأمريكية، وأن صاحبها الأمريكي الجنسية لم يسبق له التردد على مصر ومازالت البطاقة بحوزته .

وفي كمين أعد سلفاً لهذا الغرض تم ضبط كل من :

- هـ . أ . ع محام ومقيم بالجيزة
- أ . م . س صاحب محل قطع غيار سيارات ومقيم بالقاهرة حال ترددهما على محل المفروشات بالمركز التجاري وضبط مع الأول كمية من إشعارات الخصم خاصة بذات المحل وثلاث بطاقات باسم المتهم صادرة من بنك مصر، وبفحصهما فنيا بالإدارة تبين أن شريطهما الممغنط ملقن ببيانات بطاقة أخرى منسوبة للمؤسسة الأمريكية المشار إليها .

بمواجهة المتهمين أنكر الثاني صلته بالواقعة بينما اعترف الأول بحيازته للمضبوطات وسابقة تردده على ذات المحل ومحال أخرى لشراء مفروشات وأجهزة وأثاث بموجب تلك البطاقات المزورة، وأضاف أنه يتحصل عليها من آخر يدعى م.م.ع، حيث أشارت التحريات اللاحقة إلى أن الأخير طالب بكلية الطب ومقيم بالهرم، وأنه استغل اتقانه في التعامل مع الحاسب الآلي وشبكة الانترنت في الولوج إلى العديد من مواقع القرصنة على شبكة الانترنت، وسرقة بيانات البطاقات الائتمانية الخاصة بالغير وتلقينها لبطاقات مزورة أو خاصة بآخرين لاستخدامها في تمويل عمليات شراء من المحال التجارية داخل مصر.

عقب استئذان النيابة العامة تم ضبط الأخير وعثر بمسكنه على ما يلي:

١ ـ جهازي حاسب آلي أحدهما نقال.

٢ ـ كمية من إشعارات الخصم خاصة ببطاقات ائتمانية عديدة وكذا العديد من قسائم تحويل الأموال المنسوبة لمؤسسة «ويسترن يونيون» تفيد تحويل مبالغ مالية لآخرين بالخارج.

٣ ـ جهاز قراءة وتكوير البيانات على الأشرطة الممغنطة للبطاقات.

٤ ـ مجموعة من بطاقات الخصم باسم المتهم وملقنة لبيانات لبطاقات أخرى.

٥ ـ مجموعة من الأقراص المدمجة CDs.

٦ ـ أربعة هواتف محمولة حديثة لماركات مختلفة وسيارة ماركة أوبل حديثة من متحصلات لنشاط المتهم.

جانب من مضبوطات القضية

وبتفتيش مسكن المتهم الأول عثر بحوزته على كميات من الأجهزة والسلع المعمرة والأثاث الحديث واللوحات الزيتية الثمينة تم شراؤها حديثا بموجب البطاقات المزورة، وكذا سيارة ماركة ستروين حديثة من متحصلات النشاط أيضاً.

وبفحص جهازي الحاسب الآلي والأقراص المدمجة تبين أنها تحوي :

١ ـ أعداداً كبيرة من الملفات بعضها يحوي أعداداً هائلة من أرقام بطاقات الدفع الإلكتروني المنسوبة لبنوك في العديد من دول العالم.

٢ ـ أعداداً كبيرة من الرسائل داخل صندوق البريد الإلكتروني الخاص بالمتهم تفيد تبادله لكميات هائلة من أرقام البطاقات المنسوبة للعديد من البنوك والمؤسسات المالية في دول العالم المختلفة منذ عدة سنوات.

٣ ـ أمكن حصر ما يزيد على ٥٠,٠٠٠ خمسين ألف رقم بطاقة فيزا وأعداد كبيرة منها مقترن بالأرقام السرية الخاصة بأصحابها.

٤ ـ مجموعة كبيرة من برامج وأدوات القرصنة على شبكة الانترنت، مما تساعد على اختراق المواقع والشبكات من خلال استغلال نقاط الضعف في أنظمة التشغيل في أجهزة الشركات.

٥ ـ مجموعة من الملفات تفيد ارتباط المتهم بعلاقات واسعة مع آخرين من خلال غرف الدردشة والمجموعات الإخبارية على شبكة الانترنت.

وبتطوير مناقشة المتهم الأخير م. أ. ع. اعترف بنشاطه في تزوير بطاقات الدفع الاليكتروني باستخدام وحدة التكويد المضبوطة بحوزته، وأضاف أنه يقوم بدور الوساطة في بيع وتداول أرقام وبيانات بطاقات الدفع الإلكتروني الخاصة بالبنوك والمؤسسات المالية على الشبكة الدولية نظير مبلغ يتراوح بين اثنين إلى خمسة دولارات أمريكية للبطاقة الواحدة، يتم إيداعه في حساب خاص به، قام بفتحه لهذا الغرض على موقع إحدى المؤسسات المالية بالشبكة الدولية، ويقوم بصرف ما يحتاج إليه من مبالغ من ذلك الحساب باستخدام بطاقة صرف نقدي E-gold من آلات السحب النقدي المنتشرة داخل مصر أو خارجها.

تم إخطار المنظمة الدولية للشرطة الجنائية وكذا مؤسستى فيزا وماستر كارد بأرقام البطاقات وأسماء المواقع التي يرتادها المتهم للتعامل معها فنياً ومصرفياً.

باشرت النيابة العامة التحقيق وأمرت بحبس المتهمين الثلاثة احتياطياً على ذمة القضية إلى أن تمت إحالتها لمحكمة جنايات القاهرة التي أصدرت حكمها بالسجن المشدد على المتهم الأخير م. أ. ع لمدة ست سنوات والمتهم الأول بالسجن لمدة عامين بينما تم استبعاد المتهم الثاني من الاتهام.

بيان بأهم المواقع التي كان يستخدمها المتهم الأول في اختراق البنوك والمؤسسات المالية بدول العالم المختلفة وتجميع حصيلة نشاطه وصرفها من القاهرة

القضية الثالثة: تصيد

سرقة بيانات بطاقات الدفع الإلكتروني بطريق التصيد Phishing واستخدامه في تمويل عمليات شراء أو سحب أو تحويلات نقدية.

تبلغ من المنظمة الدولية للشرطة الجنائية Interpol بما ورد من انتربول واشنطن بتعرض شركة ويسترن يونيون «وهى مؤسسة مالية متخصصة في تحويل الأموال بين دول العالم المختلفة للاحتيال وذلك من مواطنين في عدة دول من بينها مصر والأردن والإمارات العربية المتحدة، تونس، تركيا،

رومانيا» وقاموا بإجراء تحويلات نقدية بواسطة خدمة تحويل الأموال التي تقدمها الشركة من خلال موقعها على شبكة الانترنت، باستخدام أرقام بطاقات ائتمان تحصل عليها المتهمون من خلال رسائل بريد اليكترونية خادعة . . وقد أرفق ببلاغ انتربول واشنطن عدة كشوف تتضمن المعلومات الفنية للعمليات الاحتيالية التي تم إجراؤها بالأسلوب المشار إليه .

بمراجعة إدارة العمليات بشركة ويسترن يونيون بالقاهرة، أمكن تحديد بيانات عدد ثلاث مئة وستين عملية تحويل أموال لفروع الشركة بمصر بلغ إجمالها مئتين وثلاثين ألف دولار أمريكى، كل تحويل يقترب من الألف دولار تقريبا، وتم صرفهم بالفعل بمعرفة العديد من الأشخاص مقيمين في إحدى عشرة محافظة .

وقد أسفرت عمليات التحريات الميدانية المصحوبة بنتائج الفحص الفنى والتتبع الإليكترونى العكسى لتلك العمليات على أن وراء كل تلك الحالات مجموعة من العناصر النشطة من محترفي القرصنة على شبكة الانترنت أمكن تحديدهم .

بعد تقنين الإجراءات تم ضبط سبعة أفراد منهم بمحافظات القاهرة، والدقهلية والإسكندرية وضبط بحوزة بعضهم أجهزة الحاسب الآلي التي استخدمت في إجراء تلك العمليات ومجموعة من بطاقات الدفع الإلكتروني « بطاقات خصم من نوع E- gold وإخطارات صادرة عن بعض شركات البريد» بوصول طرود من الخارج باسم أحد المتهمين عن عمليات تمت باستخدام بطاقات ائتمانية خاصة بأجانب، وكذا كمية كبيرة من الكتب والمراجع الأجنبية وبرامج الحاسب الآلي الثمينة التي قام المتهم نفسه بشرائها من العديد من المواقع على شبكة الانترنت باستخدام أرقام بطاقات ائتمانية خاصة بأجانب .

وبفحص أجهزة الحاسب الآلي المضبوطة تبين أن كلا منها محمل بما يلي :

١ ـ أعداد ضخمة من بيانات بطاقات الدفع الاليكتروني والرقم الشفرى الخاص بكل بنك Algorithm .

٢ ـ مجموعة من الصفحات المصطنعة والمنسوبة لبعض المؤسسات المالية الأمريكية الكبرى « استخدمها المتهم كرسائل بريدية خادعة بهدف الحصول من خلالها على أرقام البطاقات الائتمانية الخاصة بمرتادي الشبكة وهو الأسلوب الذي يطلق عليه التصيد Phishing .

٣ ـ عدة آلاف من عناوين البريد الإلكتروني الخاصة بمستخدمي شبكة الانترنت المستهدفين .

٤ ـ برنامج خاص بإعادة تخليق الأرقام الصحيحة لبطاقات الدفع الإلكتروني المنسوبة للعديد من البنوك الأمريكية .

٥ ـ وبمواجهة المتهمين اعترف كل منهم بنشاطه وقيامه باستلام المبالغ المالية التي قام بتحويلها لنفسه أو لآخرين من خلال موقع شركة ويسترن يونيون على شبكة الانترنت .

٦ ـ تحرر عن الواقعة المحضر اللازم وباشرت النيابة العامة التحقيق وأمرت بحبس المتهمين احتياطياً على ذمة القضية .

هذا وبتطوير مناقشة المتهمين في تلك الوقائع اتضح أنهم قد اتخذوا كل وسائل القرصنة والتخفي والخداع أثناء ممارسة نشاطهم وحتى يصعب التوصل إليهم وذلك على النحو التالي :

١ ـ مرحلة التصيد Phishing

أ ـ تصميم صفحات مقلدة منسوبة لأحد البنوك والمؤسسات المالية وغالباً بلغة البرمجة Php تطالب المستخدم بتحديث بياناته الشخصية والمصرفية.

ب ـ التقاط عدة آلاف من العناوين البريدية الإلكترونية E-mails من بعض المواقع الشهيرة على شبكة الانترنت.

جـ ـ استهداف أصحاب تلك العناوين بمجموعة من الرسائل البريدية الخادعة المنسوبة لبعض المؤسسات والبنوك وطلب البيانات الشخصية، وبيانات بطاقة الدفع الإلكتروني والرقم السري.

د ـ قد ينخدع في تلك الرسائل بعض مستخدمي الشبكة، ولدى قيامهم بالاستجابة بالرد عليها تصل البيانات المطلوبة إلى الـ Phisher «الصياد» وليس البنك

هـ ـ غالباً ما يتم بيع هذه البيانات أو تبادلها مع منافع غير مشروعة أخرى من خلال بعض غرف الدردشة على شبكة الانترنت ومن أشهرها

- Carder Planet , Shadow crew , CC power

ب ـ مرحلة السرقة من ويسترن يونيون

أ ـ استخدام أحد مواقع خدمة البروكس Broxi server (*) لاختيار رقم تعريفي «IP»من الأرقام المخصصة للولايات المتحدة الأمريكية،

(*) خدمة البروكسي BroxiServer تقدم كخدمة مشروعة كفلتر لحجب بعض المواقع والسماح بالبعض الآخر، وقد لجأت العديد من الدول لهذه الخدمة في بداية تشغيل شبكة الانترنت، إلا أن هذه الخدمة تستخدم اليوم بصورة غير مشروعة. حيث تقدم بعض المواقع هذه الخدمة في عمليات الخداع والتخفي أثناء تصفح شبكة الانترنت مقابل مبالغ مالية بسيطة يتم سدادها عن طريق بطاقات الدفع الالكتروني

ثم تعديل هذا الرقم داخل برنامج Explorer الخاص بتصفح الانترنت على جهاز الحاسب، ليبدو وكأن المستخدم يتصفح الشبكة من داخل الولايات المتحدة الأمريكية.

ب ـ التحقق من صحة هذه الخدمة عن طريق موقع تحديد الأماكن http://www.ip2location.com وهذا الموقع يظهر للمستخدم الرقم التعريفي الخاص به وموقعه.

جـ ـ الدخول على موقع ويسترن يونيون http://www.westernunion.com وطلب تحويل مبلغ أقل من ألف دولار باستخدام رقم بطاقة الدفع الإلكتروني الذي تم سرقته من آخرين عن طريق الـ Phishing في المرحلة الأولى حيث سيظهر للمستخدم رقم الكونترول MTCN وهي اختصار Money Transfer Control Numbs يتطلب الأمر هنا في هذه الخدمة ضرورة تأكيد طلب التحويل عن طريق الاتصال التليفوني بقسم خدمة العملاء بشركة ويسترون يونيون بالولايات المتحدة حيث سيطلب موظف الشركة من المتصل رقم الكونترول والاستفسار منه عن بعض البيانات الخاصة بصاحب البطاقة المحولة منها.

د ـ ولإتمام(*) هذه المرحلة يقوم المنتحل بالدخول على احد مواقع الاتصالات وأشهرها موقع http://wwwskype.con والحصول على رقم هاتف داخل الولايات المتحدة وهذه الخدمة للاستقبال فقط.

(*) تتيح شركة ويسترن يونيون هذه الخدمة للمواطنين والمقيمين داخل الولايات المتحدة الأمريكية فقط، حيث يمكن لأي منهم الدخول إلى الموقع وتحويل مبلغ في حدود الألف دولار شهرياً لآخرين في عدة دول من بطاقته الائتمانية.

هـ- الدخول على أحد مواقع خدمات الاتصالات الأخرى التي تسمح بتغيير رقم الهاتف المتصل (وأشهرها موقع http:// www.spooftel.com . و http://www.spoofcorcl.com وطلب تغيير رقم الهاتف الذي سبق له الحصول عليه في البند السابق مع استخدامه في خدمة الاتصال بهدف تغيير الرقم الذي سيظهر لدى موظف الشركة وتمهيداً للاتصال بـ شركة ويسترن يونيون ليبدو المتصل كأنه يتصل من داخل الولايات المتحدة (وهو في الحقيقة يتصل من داخل مصر أو أي دولة أخرى) .

و- الدخول على موقع http://www.peoplefinder.com [1] للحصول على البيانات الشخصية الخاصة بصاحب البطاقة مثل اسم الأم ومحل الإقامة السابق أسماء الأقارب . . . إلخ .

ز- الدخول على موقع http://www.spooftel.com وإجراء الاتصال بعد التأكد من تغير الرقم برقم هاتف شركة ويسترن يونيون لتأكيد التحويل .

وفي هذه الحالة سوف يطلب موظف الشركة من المتصل رقم الكونترول الذي حصل عليه من موقع الشركة ثم التحقق من شخصية المتصل من خلال عدة أسئلة يتولى المتصل « المحتال » الرد عليها من خلال ما حصل عليه من معلومات من خلال موقع http://www.peoplefinder.com ويتم التحويل

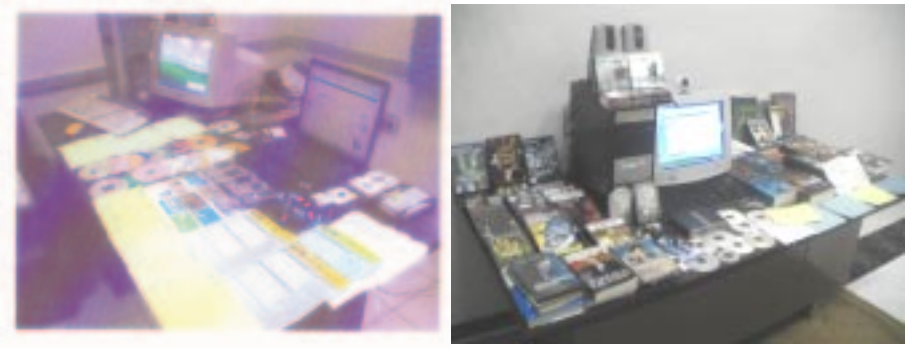
وقد اتضح من خلال فحص ومتابعة العديد من الحالات التي تم ارتكابها بذات الأسلوب عدم وجود ارتباط أو اتفاق بين مرتكبي تلك العمليات إلا

---

(١) هذا الموقع يحتوي على بيانات الأحوال المدنية لكل مواطني الولايات المتحدة الأمريكية والمقيمين بداخلها .

في حالات قليلة وان العناصر النشطة في هذا المجال قد لا يعرف كل منهم الآخر إلا من خلال الاسم المستعار داخل غرفة الدردشة في شبكة الانترنت.

جانب من مضبوطات قضيتي تصيد واحتيال ضمن مشروع (Gold Phish)



٥ .٣ جرائم موظفي مراكز البطاقات

هذا النوع من الجرائم «رغم انتشاره» إلا أنه من الصعب اكتشافه وتحديد أشخاص مرتكبيه، ويعكس ضعف وسائل وأدوات الرقابة الداخلية لدى بعض البنوك، وكثيراً ما تسعى البنوك إلى التسوية مع العميل «الضحية» أو المتضرر دون اتخاذ أي إجراءات قانونية قبل الموظف المتورط في مثل تلك الوقائع، والاكتفاء بالجزاء الإداري أو إنهاء الخدمة وعدم الإعلان عن تلك الوقائع حفاظاً على السمعة، ونعرض هنا نماذج لبعض تلك القضايا.

القضية الأولى :علميات احتيالية

تبلغ من البنك «ع.ا.د» باكتشاف تعرض البنك لعمليات احتيالية ترتب عليها تحمل البنك لخسائر تجاوزت المائتى ألف جنيه من خلال مركز البطاقات.

وقد اتضح من الفحص الفنى الذى أجري بمعرفة الإدارة بالتنسيق مع قطاع نظم المعلومات لدى البنك أن تلك المبالغ قدتم الاستيلاء عليها وصرفها من خلال عمليات فنية معقدة داخل مركز البطاقات، وأن وراء تلك الوقائع أحد موظفي صيانة وحدات البيع الإلكترونية POS لدى التجار ويدعى «أ. س. م» حيث قام الأخير بالاتفاق مع آخرين من خارج البنك، حيث تقدما للبنك وحصلا على بطاقتي دفع إلكتروني VISA، ثم يقوم الموظف المذكور حال تردده على بعض المحلات المتعاقدة لدى البنك لإجراء عمليات الصيانة الدورية للوحدات الإلكترونية POS بمغافلة المسئولين بتلك المحلات، وإجراء عمليات ارتجاع عكسية من خلال تلك الوحدات لبعض المشتريات «الوهمية» إلى أرقام بطاقات الدفع الإلكترونية الخاصة بشريكيه، ليتوليا بعد ذلك صرف تلك المبالغ من خلال آلات الصرف الآلي المنتشرة بالقاهرة.

تم وضع الموظف المذكور تحت المراقبة والتحريات المستمرة التي أسفرت عن ضبطه حال ارتكابه لواقعة مماثلة، وبمواجهته اعترف بنشاطه وأرشد عن شريكيه، فتم ضبطهما وباشرت النيابة العامة التحقيق وأمرت بحبس الثلاثة.

القضية الثانية :خصم من الأرصدة

وردت معلومات تتضمن تعرض أرصدة بعض عملاء بنك «هـ. م» للاحتيال عن طريق خصم مبالغ مالية من أرصدتهم لدى البنك نتيجة عمليات شراء أجهزة وبضائع باستخدام بطاقات منسوبة لهم، لم تسلم إليهم، الأمر الذى دفع بعضهم إلى اللجوء للقضاء في مواجهة مسئولي البنك.

أسفر الفحص الفني الذي أجري بمعرفة الإدارة بأن معظم تلك العمليات تمت من خلال محلات شهيرة بالمعادي والهرم.

بعد التنسيق مع مسئولي الأمن بتلك المحلات وفي كمين أعد لهذا الغرض تم ضبط كل من :

- ح.س.ع : ويعمل بالمكتب الهندسي للاستشارات الهندسية.
- ع.س.ع : موظف إداري بالبنك المشار إليه (شقيق الأول).

حال قيام الأول بشراء جهاز تليفون محمول «ماركة نوكيا» قيمته ثلاثة آلاف جنيه باستخدام بطاقة ائتمانية منسوبة لذات البنك تحمل صورته وبيانات أحد عملاء البنك. . وبتفتيشه عثر معه على بطاقتي ائتمان تحملان صورته وبيانات أشخاص آخرين من عملاء ذات البنك.

وبمواجهته بما أسفرت عنه التحريات اعترف بارتكابه للواقعة مستغلاً خبرته وسابقة عمله أثناء تعاقد الشركة التي يعمل بها مع البنك في طباعة وإصدار بطاقات الائتمان لعملاء البنك وأضاف بقيام زوجته ع. س.ع وشقيقه اللذين يعملان بالبنك بنفس مركز إصدار البطاقات بإمداده ببيانات تلك البطاقات والحد الائتماني لها حتى يسهل استخدامها بالمحلات التجارية.

عقب تقنين الإجراءات تم ضبط الأخيرة. وبتفتيش مسكن المتهمين عثر على ما يلى :

١ ـ عدد (١٧٠) بطاقة ائتمانية (ماستر كارد) خاصة بذات البنك وبفحصها تبين عدم طباعتها بالأرقام البارزة، رغم أنها محملة ببيانات وأرقام بطاقات خاصة بعملاء البنك على الشريط الممغنط وتحمل صورة أشخاص مختلفة.

٢ ـ بطاقة كارت فيزا إليكترون صادر من بنك س باسم شخص آخر .

٣ ـ أربعة أجهزة كمبيوتر بملحقاتها .

٤ ـ طابعتين ماركة H.P .

٥ ـ مجموعة كبيرة من الأقراص المدمجة (سى دي) محمل عليها العديد من البرامج التي يستخدمها المتهمون في نشاطهم .

٦ ـ كاميرا فيديو ماركة «سوني » وكاميرا تصوير ماركة « ياشكا »

٧ ـ مبلغ ١٠٩٩٥٠ جنيها وعدد (١٥) جنيهاً ذهبياً وايصال إيداع بمبلغ ١٠٠ ألف جنيه باسم المتهم ح . س . ع بحسابه ببنك م « فرع محمد فريد » وعدد ثلاثة دفاتر توفير خاصة بأبناء المتهم الثاني بها مبلغ ٢٠٤٥٠ جنيه .

٨ ـ بفحص أجهزة الكمبيوتر بوحدة الفحص الفني بالإدارة تبين أنها محملة بالعديد من الملفات التي تحوي كميات هائلة من بيانات بطاقات الائتمان الخاصة بعملاء ذات البنك وبنك «س» وبرامج إصدار وطباعة تلك البيانات على البطاقات .

٩ ـ بمواجهة المتهمين اعترفوا بنشاطهم بتزوير بطاقات الائتمان ببيانات عملاء بنك هـ . م باستخدام بطاقات خام مستولى عليها من البنك وطباعتها باستخدام أجهزة طباعة وأدوات التكويد المغنطة بمركز البطاقات ببنك س بمعرفة المتهم الأول مستغلا طبيعة عمله لدى الشركة المكلفة بتنفيذ عمليات طباعة وإصدار البطاقات لدى البنك .

١٠ ـ تبين ارتكاب المذكورين للعديد من وقائع شراء البضائع والأجهزة من العديد من المحلات تم فحصها بالتنسيق مع إدارتي البنكين والمحلات التجارية .

١١ ـ تحرر بشأن تلك الواقعة المحضر اللازم للعرض على النيابة التي أمرت بحبس أفراد التشكيل .

١٢ ـ تم تحديد الثغرات الفنية والإدارية لدى قطاعي البطاقات بالبنكين وتقدير حجم الأخطار الناجمة عنها ومخاطبة البنك المركزي المصري بها لتلافيها مستقبلا حفاظا على المال العام .

جانب من المضبوطات

الخاتمـــة

وأخيرا فإنه يمكن لنا أن نستخلص من هذه الدراسة النتائج التالية :

أولاً : كشفت الدراسة عن وجود قصور تشريعي واضح في هذا النوع من الجرائم ، خاصة ما ارتبط منها بتكنولوجيا المعلومات ، رغم اتجاه العديد من دول العالم المتقدم منها والنامي بسد الجوانب التشريعية في هذا المجال .

ثانياً : كشفت الدراسة عن وجود قصور معرفي واضح بهذا النوع من الجرائم والسمات الخاصة التي تميزها ، وذلك لدى العديد من أجهزة الشرطة ، خاصة ما ارتبط من تلك الجرائم بتكنولوجيا المعلومات والاتصالات ، الأمر الذي يزيد من صعوبة ملاحقة تطورها مستقبلاً

ثالثاً : إن ما أمكن الحصول عليه من بيانات حصرية عن هذا النوع من الجرائم لا يعكس بالضرورة حجم هذا النشاط في الواقع ، نظرا لإحجام العديد من الضحايا أفراداً أو مؤسسات عن الإبلاغ عن تلك الوقائع حفاظاً على السمعة ، كما أن العديد من الضحايا قد اعتادوا على عدم مراجعة كشوف الحساب الخاصة بهم بعناية .

رابعاً : صعوبة إمكانية حصر نطاق هذا النشاط داخل حدود الدول ، في ظل تطور تكنولوجيا الاتصالات والمعلومات .

خامساً : عدم وجود أجهزة أو وكالات متخصصة في الاستعلام الائتماني أو المصرفي تتولى إمداد البنوك والمؤسسات المالية بالمعلومات الكافية عن حاملي البطاقات أو التجار ذوى التاريخ والسمعة السيئة في هذا المجال ، لدى العديد من الدول العربية[1] .

(١) تعتمد البنوك والمؤسسات المالية فى غالبية دول العالم المتقدم على تلك الوكالات التي تسمى

سادساً: ضعف التعاون الأمني والقضائي على المستوى الدولى رغم أهميته القصوى في مواجهة هذا النوع من الجرائم.

وأخيرا فإننا نوصي بما يلى:

١ ـ ضرورة الإسراع في معالجة القصور التشريعي في مجالات جرائم نظم المعلومات وبطاقات الدفع الاليكتروني.

٢ ـ ضرورة تخصيص فريق عمل من الضباط والمتخصصين في كل دولة لمواجهة هذا النوع من الجرائم مع الاهتمام بتدريبهم ورفع كفاءتهم بصورة مستمرة.

٣ ـ العمل على دراسة معاهدة بودابست لمكافحة جرائم المعلوماتية، ودراسة إمكانية انضمام الدول العربية إليها، للاستفادة مما تتيحه هذه الاتفاقية من تسهيلات في مكافحة هذا النوع من الجرائم على المستويين الدولي والعربي.

٤ ـ تفعيل الاستفادة مما تتيحه منظومة اتصالات منظمة الانتربول (I-24/7) في تعزيز التعاون وتبادل المعلومات وتتبع البيانات حول مرتكبي هذا النوع من الجرائم على المستويين العربى والدولى.

٥ ـ ضرورة حث وتشجيع أجهزة المكافحة في كافة الأقطار العربية على المشاركة الفعالة في المؤتمرات والندوات التي تقام في هذا الصدد في الأوساط الأمنية، أو المصرفية والمالية، بل والدعوة إلى عقدها بصورة دورية، وذلك بهدف خلق البيئة المناسبة التي تسمح بتبادل الخبرات في هذا المجال

٦ ـ ضرورة وجود نوع من التنسيق بين البنوك والمؤسسات المالية المصدرة لبطاقات الدفع الإلكتروني والأجهزة الأمنية المختصة على المستوى الوطنى.

٧ـ حث وتشجيع البنوك والمؤسسات المالية العاملة في هذا المجال في كافة الأقطار العربية للعمل على مسايرة التحولات التكنولوجية العالمية خاصة فيما يتعلق بالحلول الفنية في مواجهة هذا النوع من الجرائم، كالتوسع في تطبيقات البطاقات الذكية Smart Cards والتوقيع الإلكتروني.

٨ـ دفع البنوك والمؤسسات المالية إلى ضرورة الاهتمام بتثقيف وتوعية عملائها للحيلولة دون وقوعهم ضحايا هذا النوع من الجرائم، وذلك من خلال نشرات التوعية المطبوعة المرسلة مع كشوف حساباتهم الشهرية.

٩ـ دفع البنوك والمؤسسات المالية بضرورة العمل على الالتزام بتطبيق المعايير التي تفرضها المؤسسات الدولية المعنية بنظم بطاقات الدفع الإليكترونى، خاصة فيما يتعلق بإجراءات الرقابة داخل مراكز الإصدار الخاصة بتلك البنوك، للحد من صور الانحراف الوظيفي في هذا المجال.

١٠ـ ضرورة العمل على وجود صيغة من صيغ التعاون العربي أمنيا وقضائياً ومصرفياً لمواجهة هذا النوع من الجرائم.

المراجـــع

اولا: مراجع قانونية وعلمية

بسيوني، محمود شريف (٢٠٠٣م). الجريمة المنظمة وغسل الأموال في القانون الجنائي من إصدارات معهد سيراكونها الدولى، ايطاليا .

بصلة، رياض فتح الله (١٩٩٥م). جرائم بطاقات الائتمان، دار الشروق، القاهرة .

الحبوش، طاهر خليل (٢٠٠١م). جرائم الاحتيال، الأساليب والوقاية والمكافحة، من إصدارات مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض .

الرهوان، محمد حافظ (٢٠٠٠م). النقود والبنوك والأسواق المالية، طبعة، بدون ناشر .

سرور، أحمد فتحى(١٩٨٨م). الوسيط في قانون العقوبات « القسم الخاص » ط ٣، دار النهضة العربية .

الشوا، محمد سامي (١٩٩٨م). ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة .

الصغير ، جميل عبد الباقي (٢٠٠١م). الإنترنت والقانون الجنائي، دار النهضة العربية .

طاهر، مصطفي (٢٠٠٢م). المواجهة التشريعية لظاهرة غسل الأموال، دار نهضة مصر، القاهرة .

عبد الحكم، سامح محمد (٢٠٠٣م). الحماية الجنائية لبطاقات الائتمان، دار النهضة العربية .

هرجة، مصطفي مجدي (١٩٩٢م). التعليق على قانون العقوبات في ضوء الفقه والقضاء، ط ٢، نادي القضاة المصري .

ثانيا : دراسات وبحوث

أرشيف الإدارة العامة لمباحث الأموال العامة، وزارة الداخلية، القاهرة.

عابد ، وسام (٢٠٠٦م). الاحتيال الإلكتروني فن ومحاربته علم، ورقة عمل مقدمة لمؤتمر مستقبل الدفع الإلكترونى، دبى .

عبد المتعال، عمرو زكي (٢٠٠٢م). المعاهدة الدولية لمقاومة جرائم الحاسبات، ورقة عمل مقدمة لمؤتمر الجوانب القانونية للتجارة الإلكترونية، جامعة الدولة العربية، القاهرة.

عساف، فاليري (٢٠٠٦م). إجراءات ومعايير الرقابة داخل مراكز البطاقات منتدى مكافحة الاحتيال، مكتب منظمة الفيزا العالمية، القاهرة.

عطية، عطية سالم (١٩٩٨م). التعريف بنظام بطاقات الدفع الإليكترونى، دراسة مقدمة لندوة الصور المستحدثة لجرائم بطاقات الدفع الإليكترونى، مركز بحوث الشرطة، أكاديمية الشرطة، القاهرة .

فهيم، فهيم كامل، المرجع العملي لأعمال إدارة أخطار بطاقات الائتمان، البنك الأهلى المصري، قطاع بطاقات الائتمان.

فوزي، نجاح محمد (١٩٩٧م). الاحتيالات المصرفية، أنواعها وأساليب مكافحتها، دراسة مقدمة للمؤتمر العربي التاسع لرؤساء المباحث والأدلة الجنائية، تونس .

مجتمع اللانقود (٢٠٠٦م). من إصدارات منظمة الفيزا العالمية، القاهرة.

ثالثا : مواقع متخصصة على شبكة الإنترنت

http:// www:intenetworldstats.com

http:// www internetworldstats.com/stats.htm

http:// www.internetworldstats.com

http:// forum.carderplanet.net.

http://www.usdoj.gov/ usao/press/ html/2004.

http://www.papacs.org.uln

http://www.westernunion.com/history.

http://www.nilsonreport.com

http://www.citybank.com

http://www.visa.com

Http://en.wikipedia.oirg/wikilchip-card

http://www.primarykey.co.uk

http://www.emvco.com

http://www. globalplatform.org

http://www.forrester.com

http:// www.inerimentalgold.com

http://www.paypal.com

http:// www.westernunion.com

http:// www.moneypram.com

http://thecreditcardgenerators.com.

http://www.kanecal.net/mag-stripe

http://stor.aiallc.com.

http://hackershomepage.com.

https://www.interpol.int

http://www.snopes.com./fraud/atm
http://en.wikipedia.org.
http://office.microsoft.com
http://www.usdoj.gov/usao/cmn/press
http://www.symantec.com
http://www.gotrack.us/congress
http://www.egovs.com
http://www.lob.gov.go/ui/laws
http://www.gcc-legal.org
http://www.justice.gov.ma
http://conventions.coe.int
http:// www.interpol.org
https://www.interpol.int .
http:// www.antiphishing.org
http:// www.microsoft.com
http://www.visa.com
http://www.gsmworld.com
http://www.complicanceandprivacy.com.